Transportation Systems

Critical Infrastructure and Key Resources
Sector-Specific Plan as input to the
National Infrastructure Protection Plan

May 2007

Homeland Security

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **MAY 2007**	2. REPORT TYPE	3. DATES COVERED **00-00-2007 to 00-00-2007**

4. TITLE AND SUBTITLE **Transportation Systems: Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Homeland Security,Washington,DC,20528**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**154**	

U.S. Department of Homeland Security
Arlington, VA 22202

Transportation Security Administration

The National Infrastructure Protection Plan (NIPP) provides the unifying structure for the integration of Critical Infrastructure and Key Resources (CI/KR) protection efforts into a single national program. The NIPP provides an overall framework for integrating programs and activities that are underway in the various sectors, as well as new and developing CI/KR protection efforts. The NIPP includes 17 sector-specific plans (SSPs) that detail the application of the overall risk management framework to each specific sector.

Each SSP describes a collaborative effort between the private sector; State, local and tribal governments; nongovernmental organizations; and the Federal Government. This collaboration will result in the prioritization of protection initiatives and investments within and across sectors to ensure that resources can be applied where they contribute the most to risk mitigation by lowering vulnerabilities, deterring threats, and minimizing the consequences of attacks and other incidents. By signing this letter, the members of the Transportation Sector Government Coordinating Council (TSGCC) commit to:

- Support the Transportation SSP concepts and processes, and carry out their assigned functional responsibilities regarding the protection of CI/KR as described herein;

- Work with the Secretary of Homeland Security and the Assistant Secretary of Homeland Security for Transportation Security, as appropriate and consistent with their own agency-specific authorities, resources, and programs, and to coordinate funding and implementation of programs that enhance CI/KR protection;

- Cooperate and coordinate with the Secretary of Homeland Security and the Assistant Secretary of Homeland Security for Transportation Security, in accordance with guidance provided in Homeland Security Presidential Directive 7, as appropriate and consistent with their own agency-specific authorities, resources, and programs, to facilitate CI/KR protection;

- Develop or modify existing interagency and agency-specific CI/KR plans, as appropriate, to facilitate compliance with the Transportation SSP;

- Develop and maintain partnerships to CI/KR protection with appropriate State, regional, local, tribal, and international entities; the private sector; and nongovernmental organizations; and

- Protect critical infrastructure information according to the Protected Critical Infrastructure Information Program or other appropriate guidelines, and share CI/KR protection-related information, as appropriate and consistent with their own agency-specific authorities and the process described herein.

At present, the Transportation Sector Coordinating Council (TSCC) is in the process of being formed, but the process is not complete. The TSGCC enthusiastically endorses the formation of the TSCC and we look forward to advancing the Transportation Sector Specific Plan together with these key stakeholders.

John P. Sammon
Co-Chair
Transportation Sector Government Coordinating Council
Transportation Security Administration
Department of Homeland Security

Robert J. Caverly
Co-Chair
Transportation Sector Government Coordinating Council
Office of Infrastructure Protection
Department of Homeland Security

Table of Contents

List of Figures

List of Tables

Executive Summary

Transportation Security Environment

The Transportation Systems Sector—a sector that comprises all modes of transportation (Aviation, Maritime, Mass Transit, Highway, Freight Rail, and Pipeline)—is a vast, open, interdependent networked system that moves millions of passengers and millions of tons of goods. The transportation network is critical to the Nation's way of life and economic vitality. Ensuring its security is the mission charged to all sector partners, including government (Federal, State, regional, local, and tribal) and private industry stakeholders. Every day, the transportation network connects cities, manufacturers, and retailers, moving large volumes of goods and individuals through a complex network of approximately 4 million miles of roads and highways, more than 100,000 miles of rail, 600,000 bridges, more than 300 tunnels and numerous sea ports, 2 million miles of pipeline, 500,000 train stations, and 500 public-use airports.

The sector's security risks are evident by attacks either using or against the global transportation network, including not only the September 11, 2001, attacks on the World Trade Center and the Pentagon, but also more recent attacks on transportation targets such as the 2005 London bombings, the coordinated attack on four commuter trains in Madrid in 2004, and the 2006 plot uncovered in the United Kingdom targeting airlines bound for the United States. These recent attacks are a sobering reminder that the transportation system remains an attractive target for terrorists post-September 11. Hurricane Katrina and other disasters (natural and industrial) also highlight the risk to the sector that is not directly related to terrorism. Taken together, the risk from terrorism and other hazards demands a coordinated approach involving all sector stakeholders.

In the wake of the September 11 attacks, the Transportation Systems Sector joined together in an unprecedented way to protect its customers, systems, and assets. The private sector has made great contributions in sector-wide risk-reduction efforts, often of their own volition. State and local governments likewise reacted swiftly to the attacks, enhancing first-response capabilities, increasing vigilance, and securing potential targets. This type of cooperation among the diverse sector stakeholders is one of the strengths of the Transportation Systems Sector.

In addition to ongoing efforts, there is a distinct set of strategic risks where the Federal Government will add special value. These risks exhibit two distinguishing characteristics: First, they present issues that raise complex implementation issues for industry, and State and local governments. Second, they have a very high materiality (i.e., very significant consequence and plausible likelihood). Strategic risks, such as the use of some element of the transportation network as a weapon of mass destruction (WMD), have a multi-jurisdictional and sector-wide effect. Therefore, Federal involvement will improve the sector's risk management posture by focusing on system-wide risk.

In the face of the reality that terrorists will continue to target the transportation network, a systems-based risk management (SBRM) strategy that lays out a strategic framework to improve the sector's risk management posture is necessary. This strategy focuses on implementing multiple layers of security to defeat and deter the more plausible and dangerous forms of attack against the Nation's transportation network. Importantly, the SBRM process is strategic in nature, yielding strategic countermeasures, and does not directly address operational or tactical plans. The National Infrastructure Protection Plan (NIPP), signed by Michael Chertoff, Secretary of the Department of Homeland Security (DHS), in June 2006, as a requirement of Homeland Security Presidential Directive 7 (HSPD-7), obligates each critical infrastructure and key resources (CI/KR) sector to develop a Sector-Specific Plan (SSP) that describes strategies that protect the Nation's CI/KR under their purview, outline a coordinated approach to strengthen their security efforts, and determine the appropriate programmatic funding levels.

The Transportation Systems SSP and its supporting modal implementation plans and appendixes establishes the Transportation Systems Sector's strategic approach based on the tenets outlined in the NIPP and the principles of Executive Order 13416, Strengthening Surface Transportation Security. The Transportation Systems SSP describes the security framework that will enable sector stakeholders to make effective and appropriate risk-based security and resource allocation decisions.

To be effective, a strategic plan must define a vision and mission statement, coupled with targeted goals and objectives to which operational and tactical efforts are anchored. Section 1 of the Transportation Systems SSP provides a robust discussion of how the sector's security vision, mission, goals, and objectives were developed and agreed to by the sector's security partners through the Government Coordinating Council (GCC)/Sector Coordinating Council (SCC) framework.

Vision Statement:

Our vision is a secure and resilient transportation network, enabling legitimate travelers and goods to move without undue fear of harm or significant disruption of commerce and civil liberties.

Mission Statement:

Continuously improve the risk posture of the Nation's transportation system.

Goals:

1. ***Prevent and deter acts of terrorism using or against the transportation system;***
2. ***Enhance the resilience of the transportation system; and***
3. ***Improve the cost-effective use of resources for transportation security.***

The vision and mission statement for the Transportation Systems Sector establish a foundation upon which the sector's prioritization and resource allocation processes are built. The risk-informed, decisionmaking process, detailed in sections 3 through 5, outlines how strategic risk objectives (SRO) developed through the GCC/SCC framework will be formulated, continuously evaluated, and updated to reflect shifting priorities or changes in the security environment.

A Systems-Based Risk Management Approach to Transportation Security

The NIPP defines risk as a function of threat, vulnerability, and consequence. Analysis of risk and the evaluation of countermeasures require consideration of all three variables. The Transportation Systems Sector is a complex network with six interdependent modes. Disruptions in the transportation network can often have nonlinear effects. As a result, what may initially appear as an isolated disturbance in the network can have a much greater, sector-wide impact.

One of the critical challenges facing the Transportation Systems Sector is understanding the downstream implications of potential disruptions. For example, following the September 11 attacks, the aviation system was shut down and the borders were closed, causing supply chain disruptions across multiple industries. Recognizing the importance of systems is key when determining cost-effective countermeasures. Since resources available for protecting CI/KR are discretely limited, a robust decisionmaking process that provides critical information to identify the highest priority systems and assets is necessary. To meet this need, the Transportation Systems SSP outlines a structured, eight-step SBRM approach that augments the NIPP risk management framework and looks beyond protecting a single asset or set of assets. One major benefit of adopting and implementing the SBRM approach is that the sector will have a process that includes Federal, State, regional, local, and private sector experience and creativity to leverage limited resources and develop countermeasures.

Introducing SBRM does not represent a sudden change of course. Rather, SBRM focuses on a collaborative and comprehensive sector-wide effort to protect the transportation network as a whole to augment the specific asset protection planning that is currently underway. In most cases, the efforts of the sector stakeholders will not change; however, their appreciation of how those efforts fit within the overall sector risk posture will be significantly enhanced. Introducing SBRM is a first step toward integrating a systems view with the asset-based risk management currently underway.

The eight-step SBRM process, outlined in sections 3, 4, and 5, illustrates three distinct areas of focus to achieve this aim:

- What are we focusing on?
- How do we better understand risk?
- What do we do to manage the risk?

Additionally, the SBRM will help the sector members better understand the true system-wide impact and key interdependencies contained throughout the sector in planning against a terrorist attack or natural disaster. Building on Federal, State, regional, local, and private sector programs and initiatives currently in place, this robust risk management approach entails a continuous process of managing risk through a series of actions, including setting strategic goals and objectives, assessing and quantifying risks, evaluating alternative security measures, selecting which mitigation options to undertake, and implementing and monitoring countermeasures. The SBRM methodology builds on asset-based approaches and is inclusive of current programs and initiatives.

Sector Interdependencies

The Transportation Systems Sector has significant interdependencies with many of the other critical infrastructure sectors. For instance, the Transportation Systems and Energy sectors directly depend on each other to move vast quantities of fuel to a broad range of users and to supply the fuel for all types of transportation. In addition to cross-sector interdependencies, interdependencies and supply chain implications are among the various sectors and modes that must be considered. For example, interdependencies were evident during the aftermath of Hurricane Katrina, where damaged critical infrastructure (pipelines, levees, highways, etc.) disrupted government activities and interrupted commerce flows showed that key interdependencies and supply chain implications must be viewed from a systems-based perspective as opposed to single points or independent assets.

GCC/SCC Structure and Collaboration

The NIPP requires each sector to implement a Sector Partnership Model (SPM) by establishing GCCs, consisting of Federal agencies with sector-specific security responsibilities, and SCCs consisting of private sector organizations, owner-operators, and entities with transportation security responsibilities. The Transportation Systems Sector established an overarching Transportation Systems Sector GCC in January 2006. The Transportation Systems Sector GCC includes the following Federal agencies with transportation security responsibilities: the DHS, including the Transportation Security Administration (TSA), the United States Coast Guard (USCG), and Office of Grants and Training (G&T); Department of Transportation (DOT); Department of Justice, including the Federal Bureau of Investigation (FBI); and the Department of Defense (DoD). The Transportation Systems Sector GCC is further divided into modal subcouncils (Aviation, Maritime, Mass Transit, Highway, Freight Rail, and Pipeline), which include members from a broad cross-section of government agencies.

The SCCs, following the GCC organizational structure model, are organized, or are organizing, by mode. Membership includes leading associations, as well as owner-operators and other private sector transportation entities with transportation security responsibilities. The SCC currently has efforts underway to organize an overarching Transportation Systems SCC that will interface directly with the Transportation Systems Sector GCC.

These newly formed councils will act in concert to achieve the sector's goals and objectives and continuously refine the sector's security posture through the SBRM process. Both the Transportation Systems Sector GCC and Transportation Systems SCC will work collaboratively to share security information and develop sector-wide approaches to formulating and approving sector priorities, countermeasure programs, and other decisions.

Modal Implementation Plans

As stated above, the Transportation Systems Sector is divided into six modes, each with different operating structures and approaches to security. As required by Executive Order 13416, Strengthening Surface Transportation Security, the Transportation Systems SSP includes modal implementation plans or *modal annexes* that detail how each distinct mode intends to achieve the sector's goals and objectives using the SBRM approach. Separate classified versions of all surface modal implementation plans will be developed as directed by Executive Order 13416. In developing the modal implementation plans, each modal GCC and SCC was required to collaborate in developing an implementation plan that achieves the sector's goals and objectives and identifies the following: cost-effective security programs and initiatives; current industry effective practices; security guidelines, requirements, and compliance/assessment processes; available grant programs; areas for security improvement; and a process to establish metrics for determining security effectiveness and progress toward achieving the sector's goals and objectives. Within each mode, significant actions have already been undertaken to improve the sector's risk profile. These actions include implementing industry security programs and initiatives, expanding customer awareness programs, increasing the number and visibility of security personnel, and upgrading security technology.

DHS CI/KR Protection Annual Report

The Sector CI/KR Protection Annual Report (due every July 1) is an annual requirement of the NIPP in which each sector analyzes the National Risk Profile to identify and determine applicable CI/KR security priorities. The DHS subsequently incorporates priority and resource information from all 17 CI/KR sector's annual reports to develop an umbrella National CI/KR Protection Annual Report (an overview of the annual report analysis and process is discussed in the 2006 NIPP, pp. 93-96).

The Transportation Systems Sector CI/KR Annual Report that is developed will feed into the National CI/KR Protection Annual Report.

In addition to developing and maintaining a Transportation Systems SSP that supports the NIPP goal and supporting objectives, TSA and USCG, as the Sector-Specific Agencies (SSAs) for the Transportation Systems Sector, in partnership with the SCC and GCC, will determine sector-specific priorities and requirements for CI/KR protection. TSA and USCG will submit these priorities and requirements, along with resource needs, to the DHS in the Transportation Systems Sector Annual Report to allow for a more comprehensive National CI/KR Protection Annual Report.

The annual report will provide:

- Updated sector priorities and goals for CI/KR protection that reflect the current and future-based security status of the Transportation Systems Sector;
- Transportation requirements for CI/KR protection initiatives and programs that are prioritized based on risk and overall protective value; and
- Gap analysis denoting where security programs are lacking and where additional resources are potentially needed.

Appropriations and budgeting projections for NIPP-related CI/KR funding based on the sector's goals and objectives will be included in the SSA budget request as part of the Federal budgeting process.

Intelligence Efforts

One of the key elements influencing sector risk management is intelligence. The sector recognizes the importance of having real-time, credible intelligence information from Federal, State, and local intelligence-gathering entities. Again, looking at the most recent terrorist events in particular, the foiled plot in the United Kingdom demonstrates the value and necessity of aggressive intelligence and investigative activities. The DHS, through the Office of Intelligence and Analysis, has integrated their efforts with the United States Intelligence Community to ensure continual situational awareness. These offices develop intelligence products and informational materials that inform the efforts of Federal decisionmakers, system operators, and security officials. The concerted effort aims to track potential threats, disrupt development, and focus security resources and activities, as necessary, for detection, deterrence, and prevention. The sector recognizes the importance of private industry integration into the full intelligence cycle, consisting of private industry's intelligence requirements, tasking, analysis, and dissemination. Therefore, the sector will consider establishing a joint GCC/SCC intelligence working group to better coordinate and integrate intelligence efforts with the private sector.

Challenges for the Transportation Systems Sector

The Transportation Systems Sector faces difficult challenges that the sector members must address together. Implementing a sector-wide SBRM approach will provide the mechanism to not only identify SROs, but also to improve resource allocation and security program implementation decisions. However, the sector must resolve additional challenges as it moves forward with security planning efforts, such as: (1) how the Transportation Systems Sector's SSAs—TSA and USCG[1]—can manage the anticipated challenges in preparing future annual reports due to differences in the agencies' budgeting and resource allocation process; (2) how the sector can coordinate response and recovery planning and activities; (3) how the sector can determine, coordinate, and deploy effective research and development initiatives; and (4) how progress in fortifying the sector's security posture and achieving the stated goals and objectives can best be measured.

To address the latter two challenges, the Transportation Systems Sector GCC established a Research and Development (R&D) Working Group to begin coordinating Research, Development, Test, and Evaluation (RDT&E) efforts across the sector. It is envisioned that the R&D Working Group will be comprised of leading R&D experts throughout the Federal Government and the private sector community. Their purpose will be to identify, develop, and prioritize specific R&D security needs through available and proposed technologies. In addition, a Joint Measurement Working Group has been developed to include government and private sector measurement professionals. This group will begin efforts to address the inherent difficulties in measuring and assessing the performance of security solutions by developing measurement approaches and specific metrics to measure progress and transportation security performance. Measurements are not readily applicable in the ways that, for instance, corporations measure financial performance. Therefore, measurements do not necessarily need to be quantitative. However, sector measurement targets should be specific enough so that reasonable judgments can be made on whether the objectives have been attained.

Another key challenge is the ability to share security information through effective communication tools and mechanisms. The sheer number of stakeholders involved in securing the transportation network can lead to communication disruptions, duplication of efforts, and confusion about roles and responsibilities. As mentioned, the sector has already embraced the NIPP SPM by establishing GCCs and SCCs that provide the framework through which government (Federal, State, local, and tribal) and private sector entities can effectively communicate, coordinate, and collaborate on the sector's security priorities and strategic way forward.

Implementation

The most important aspect of a strategic plan is implementation. As the sector collectively moves forward in securing the Nation's CI/KR, sector stakeholders must work together to implement the sector's strategies and an SBRM approach to drive protection programs and initiatives identified in each mode-specific plan. The Transportation Systems SSP and modal implementation plans are

[1] The USCG, as the SSA for the Maritime Mode, will work within its own budget cycle to provide justifications and execution plans for its security programs. As a multi-mission service, the USCG's assets are used to meet requirements from across its 11 federally mandated mission-programs, one of which is Ports, Waterways, and Coastal Security. The USCG does not have a program dedicated to infrastructure protection, but is able to extrapolate and infer degrees of effort that contribute to infrastructure protection, and will use such methods in its approach to CI/KR risk management and the CI/KR Annual Report.

evolving documents that should be updated annually to reflect the continuation of agreements, changes in legislation, or changes in the sector's security posture.

1. Sector Profile and Goals

1.1 Introduction

The Transportation Systems Sector-Specific Plan (SSP) is one of the 17 sector plans required by the National Infrastructure Protection Plan (NIPP), which implements the requirements of Homeland Security Presidential Directive 7 (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection (December 13, 2003). Under HSPD-7, the Nation's critical infrastructure and key resources (CI/KR) are organized into sectors with certain Federal agencies designated as Sector-Specific Agencies (SSAs). These agencies are responsible for coordinating the protection activities of the sectors' security partners to prepare for and respond to threats that could have a debilitating effect on security or economic well-being. The Department of Homeland Security (DHS) is the SSA for the Transportation Systems Sector. The Secretary of Homeland Security has assigned this responsibility to the Transportation Security Administration (TSA) and the U.S. Coast Guard (USCG) for the maritime mode of the Transportation Systems Sector. The DHS, through TSA and the USCG, in collaboration with the Department of Transportation (DOT) and its modal administrations, and in close cooperation with their Federal, State, local, tribal, and private industry security partners, shares the responsibility for developing, implementing, and updating the Transportation Systems SSP and the supporting modal implementation plan annexes.

The Transportation Systems SSP combines the contributions of the sector's security partners in a sector-wide approach to managing the security risks within and across the transportation modes. Although the principal focus of the Transportation Systems SSP is on risk associated with terrorist threats and resilience, strategies discussed are also applicable to natural disasters and manmade hazards. The Transportation Systems SSP and its modal annexes explain how the Transportation Systems Sector will improve the security of its CI/KR—the assets, systems, networks, and functions that provide the vital services essential for the Nation's security, economic vitality, and way of life.

The national effort to improve CI/KR security also must conform to several other key Presidential Directives and Executive Orders. In conformance with HSPD-5, Management of Domestic Incidents, domestic incidents will be managed under the principles set forth in the National Response Plan (NRP) and the National Incident Management System (NIMS). The NRP explains how Federal, State, and local agencies will respond to all types of hazards. The NIMS organizational approach provides the doctrinal basis for determining and coordinating the resources necessary to manage incidents of all sizes and complexity. The NRP and the NIMS are currently undergoing a review process. This revision, fully engaging all levels of sector stakeholders, will determine the roles and responsibilities for response and recovery. In the meantime, the sector will begin the process of establishing a Response and Recovery Working Group (R&RWG) to determine how its efforts can be integrated into the NRP/NIMS review process. The National Preparedness Goal developed under HSPD-8, National Preparedness, provides specific objectives to ensure that communities are prepared for natural or human-caused disasters and terrorist attacks. Maritime mode security is specifically addressed in HSPD-13, National Strategy for Maritime Security, which underscores the importance of securing the maritime domain, developing a comprehensive national strategy, and ensuring effective and efficient implementation of strategies. As directed in Executive Order 13416, Strengthening Surface Transportation Security, the Secretary of Homeland Security leads the efforts for protection of the surface transportation modes by the facilitation and implementation of a comprehensive, coordinated, and efficient security program.

To address the threat of a novel influenza virus with pandemic potential, the President, on November 1, 2005, announced the National Strategy for Pandemic Influenza (NSPI), which outlines the approach that the U.S. government will take to prepare for and respond to an influenza pandemic. It also articulates the expectation that non-Federal entities will prepare themselves and their communities.

To translate the NSPI into effective actions, an accompanying Homeland Security Council (HSC) Implementation Plan for the national strategy identifies major roles and responsibilities for Federal departments and agencies. While the Department of Health and Human Services (DHHS) is the lead for public health, the DHS, with the lead for domestic incident management, and particularly border and transportation security, plays a pivotal role in the execution of the national response. Further planning coordination occurs between the DHS and the DHS component agencies and their Federal partners, many of which are outlined in the Transportation Systems SSP, on domestic and international transportation-related issues, specifically the departments of Transportation, State, and Defense.

Each Federal department and agency is responsible for creating and maintaining a pandemic influenza contingency plan. These plans include provisions for the protection of employees, the maintenance of essential functions and services, communications with stakeholders, and the manner in which the department will execute its responsibilities in support of the Federal response to a pandemic, as described in the HSC Implementation Plan.

The HSC Implementation Plan, which contains more than 300 action items to prepare for and respond to a pandemic, dedicates a section to the protection and continuity of CI/KR during a pandemic, including transportation. The Implementation Plan outlines several mechanisms and timelines for engaging stakeholders and providing guidance for their own contingency plans in support of the national response.

1.2 Sector Profile

The Nation's transportation network is a vast, open, accessible, interconnected system with as much as 85 percent of the transportation infrastructure in the United States owned by the private sector. The sheer size and capacity of this sector, which moves, distributes, and delivers millions of passengers and goods each year, makes it a highly attractive target for terrorists and a challenge to secure.

The Transportation Systems Sector is segmented into six key subsectors, or modes, which operate independently within both a regulated and non-regulated environment, yet are also highly interdependent. Such interdependence is a defining characteristic of the transportation system. The six modes—Aviation, Maritime, Mass Transit, Highway, Freight Rail, and Pipeline—all contribute to transporting people, food, water, medicines, fuel, and other commodities. The combined efforts of the modes play an important role in maintaining the public health, safety, and economic well-being of our Nation. Yet, each does so with unique characteristics, operating models, responsibilities, and stakeholders.

1. **Aviation** includes aircraft, air traffic control systems, and approximately 450 commercial airports and 19,000 additional public airfields. This mode includes civil and joint-use military airports, heliports, short takeoff and landing ports, and seaplane bases.

2. **Maritime** includes the wide range of water-faring vessels and consists of approximately 95,000 miles of coastline, 361 ports, more than 10,000 miles of navigable waterways, 3.4 million square miles of Exclusive Economic Zone to secure, and intermodal landside connections, which allow the various modes of transportation to move people and goods to, from, and on the water.
3. **Mass Transit** includes multiple-occupancy vehicles, such as transit buses, trolleybuses, vanpools, ferryboats, monorails, heavy (subway) and light rail, passenger rail (including both commuter rail and long-distance rail), automated guideway transit, inclined planes, and cable cars, designed to transport customers on regional and local routes.
4. **Highway** encompasses more than 4 million miles of roadways and supporting infrastructure. Vehicles include automobiles, buses, motorcycles, and all types of trucks, trailers, and recreational vehicles.
5. **Freight Rail** consists of hundreds of railroads, more than 143,000 route-miles of track, more than 1.3 million freight cars, and roughly 20,000 locomotives.
6. **Pipeline** includes vast networks of pipeline that traverse hundreds of thousands of miles throughout the country, carrying nearly all of the Nation's natural gas and about 65 percent of hazardous liquids, as well as various chemicals.

As mentioned previously, each mode of the Transportation Systems Sector, having different security and operating environments, has developed separate modal implementation plans that are included as annexes to the Transportation Systems SSP. The plans detail the characteristics of the mode, including approaches to security, industry effective practices, guidelines, assessments, and regulations. In parallel with developing the Transportation Systems SSP, the plans explain how each mode will incorporate sector goals into modal security programs.

1.2.1 Cross-Sector Dependencies

There are many dependencies and interdependencies between the various CI/KR sectors. Virtually every sector is dependent, to some degree, on the Energy, Communications, and Transportation Systems sectors. In addition, because critical sectors have different and potentially competing interdependencies, it is vitally important to determine key relationships to gain a better understanding of the overall complexities when undertaking planning and policy initiatives for critical infrastructure protection (CIP). Key dependencies are those that, if interrupted, could significantly impact the performance of the transportation system and its overall resilience.

As the following examples demonstrate, CI/KR sectors not commonly associated with transportation will be significantly impacted by a major disruption in one or more of the transportation modes.

- The Energy Sector requires coal, crude oil, petroleum products, and natural gas that are transported by ship, barge, pipeline, rail, and truck.
- The Defense Industrial Base uses the Nation's air, maritime, rail, and highway networks to move materiel in support of military operations.
- The Banking and Finance Sector and Government Services Sector rely on mass transit systems in large urban areas for employees to access the workplace.

- The Communications Sector co-locates much of its networking equipment (routers, fiber-optic cable, etc.) along existing transportation routes (rail lines, highway tunnels, and bridges), the destruction of which may impact service availability in wide geographic areas.
- The manufacturing and commercial sectors move goods and services across the entire transportation network utilizing all transportation modes.

The integrity of the Transportation Systems Sector is also directly dependent on the efforts of other sectors.[2]

- The Energy Sector produces fuels to power transportation systems.
- The Information Technology Sector is essential in the transmission of information necessary for the efficient operation of the transportation network.

In addition to cross-sector interdependencies, the Transportation Systems Sector must pay particular attention to interdependencies among the transportation modes. Those issues that affect more than one mode will be given special consideration, recognizing that many assets serve more than one mode.

As with the traditional aspects of the transportation network, interdependencies also exist between cyber assets, people, and the facilities in which they reside. To identify and prioritize these dependencies, sector members are encouraged to perform an interdependency analysis, which government agencies, private companies, and universities have developed. TSA and USCG, as the SSAs, will help sector members identify a methodology that meets their needs.

1.3 The Transportation Security Environment

Like many other critical infrastructure sectors, the Transportation Systems Sector faces a dynamic landscape of potential natural disasters, accidents, and terrorist attacks. The terrorist threat poses special challenges. While terrorists may rely on a distinct set of attack methods, they can adjust their attack strategies based on past responses. As a result, unlike natural disasters or accidents, the time and place of terrorist attacks cannot easily be predicted by just evaluating historical events. Modes of transportation have been used in terrorist attacks not only in New York and Washington, DC, on September 11, 2001, but also in London, Madrid, and Mumbai, India.

The Transportation Systems Sector is highly complex because of a number of reasons. One reason is sheer scale—the sector is composed of hundreds of thousands of assets, links, and nodes spread across the six modes. Some assets, such as airports or rail yards, are stationary. Others, such as hazardous materials (HAZMAT) trucks or commercial airplanes, are mobile and may be used as weapons, as well as targets. These assets are widely distributed geographically, in both rural and urban areas, covering all 50 States and Territories.

Secondly, the Transportation Systems Sector consists of numerous and diverse stakeholders, including Federal, State, and local government agencies, as well as private owner/operators. Owner/operators across the modes may face different decision incentives and constraints.

[2] Cross-sector working groups and simulation models via the National Infrastructure Simulation and Analysis Center (NISAC) (e.g., Critical Infrastructure Protection/Decision Support System (CIP/DSS)) will be used to further explore these interdependencies.

A third reason for the complexity that characterizes the Nation's transportation network is interconnectedness and supply chain implications among the assets and systems that comprise it. The security challenge faced by the 21st century transportation community is due, in large part, to the interconnected, interdependent network that has been created to meet the demands of the economy and of the citizens. Over the past two decades, the sector, like most other infrastructures, has expanded and altered its business models on a global scale to take advantage of the so-called "network effect."[3] While these changes have significantly enhanced the efficiency and effectiveness of the sector, they have also resulted in a more complicated operating model. The result is a transportation network that becomes more and more complex and interdependent each year.

These insights are key to understanding why the sector's mission is to enhance transportation security while maintaining the free flow of commerce. Terrorists have sought to inflict damage that is disproportionate to their efforts by attacking parts of the network that will lead to nonlinear consequences, such as a cascading failure. Additionally, terrorist threats are adaptive and dynamic in that security applied to one element of the transportation network could cause terrorists to shift their attention to other parts of the system. Therefore, the sector must simultaneously seek to improve security while minimizing the negative impact of countermeasures to ensure that macro (emergent) patterns of commerce in the transportation system are not disrupted.

1.4 Sector's Approach to Risk Management

An environment of complexity and uncertainty presents the Transportation Systems Sector with a set of challenging and sometimes conflicting decisions on how best to increase the security and resilience of the Nation's transportation network. Various stakeholders throughout the sector are actively developing methods to improve operational security and overall resilience. However, increased emphasis needs to be placed on understanding the evolving risk-based approach to security.

The Secretary of Homeland Security, Michael Chertoff, has described his vision for risk-based decisionmaking, stating "*We must manage risk at the homeland security level. That means developing plans and allocating resources in a way that balances security with freedom when calculating risks and implementing protections.*"[4]

As part of their day-to-day risk management efforts, stakeholders within the sector secure their organizations from the specific risks that threaten them. The DHS and other government entities provide the private sector with threat warning, incident reporting, and analysis whenever appropriate. Such information is critical to the sector's operational and tactical planning and implementation. Depending on the threat information, the sector may choose to adjust their operational and tactical efforts.

Due to the interconnectedness and supply chain implications of systems within the transportation network and the possibility of cascading effects from a major event, it is important to focus sector-wide efforts on strategic risks. Strategic risks are those that impact the entire sector, threatening disruption across multiple stakeholder communities. The consequences of strategic risks can also cross multiple sectors and can have far-reaching, long-term effects on our national economy, natural

[3] A characteristic that causes a good or service to have a value to a potential customer dependent upon the number of customers already owning that good or using that service.

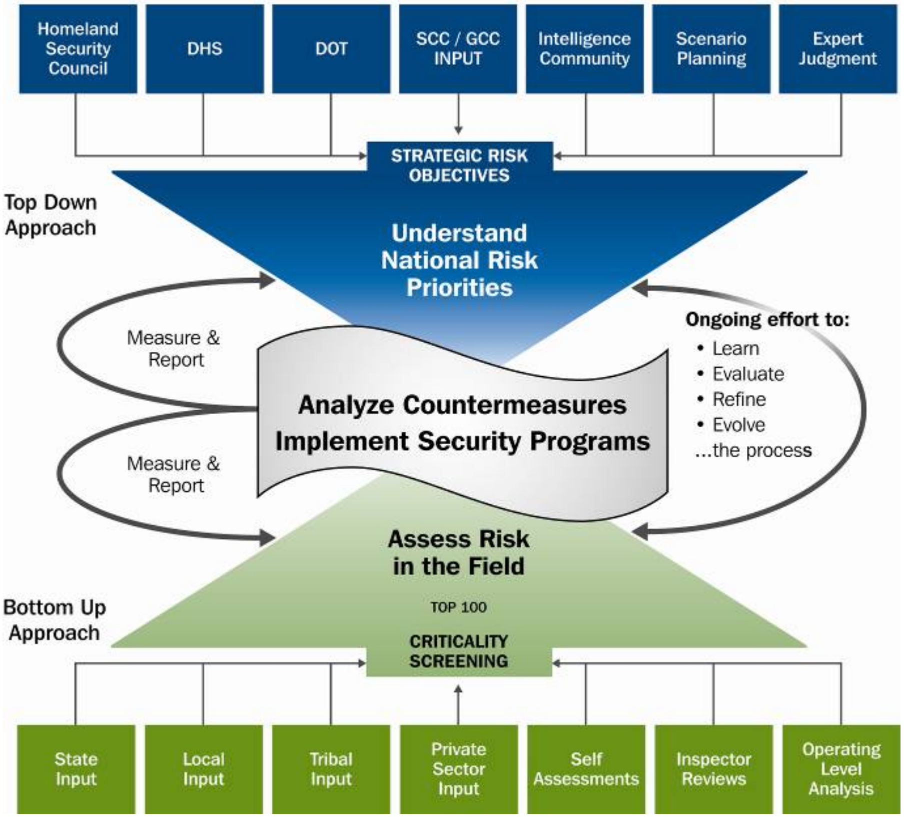
[4] Secretary of Homeland Security, Michael Chertoff, address at The George Washington University's Homeland Security Policy Institute, March 16, 2005.

environment, or public confidence. Examples of strategic risks to the Transportation Systems Sector include:

- Disruption of a mega-node[5] in the transportation network (large-scale impact on national security);
- Use of a component of the transportation network as a weapon of mass destruction (WMD) (terrorism event leading to loss of life and public confidence); and
- Release of a biological agent at a major passenger facility, such as a rail station, ferry terminal, or hub airport (terrorism event affecting national public health and safety).

Stakeholders throughout the sector have been and continue to be actively developing methods to improve their operational security and overall resilience. However, since the Transportation Systems Sector is segmented by individual modes, an increased emphasis is needed on a risk-based approach across the entire transportation spectrum. The sector's risk management approach reflects a combined top-down and bottom-up effort. Figure 1-1 illustrates the dynamic and collaborative risk assessment process and those involved in determining which risks will be identified, analyzed, prioritized, and addressed.

Figure 1-1: Integrated Top-Down, Bottom-Up Risk Assessment Cycle



[5] A mega-node refers to a single point of possible failure or bottleneck, at which multiple modes of transportation intersect, with the potential for wide-ranging disruptions and losses. An example of a mega-node is New Orleans, where all transportation modes meet and exchange goods and people. As seen in 2004, a disruption at this mega-node had wide-ranging effects on fuel, food, the movement of people, etc.

1.4.1 NIPP Risk Management Framework

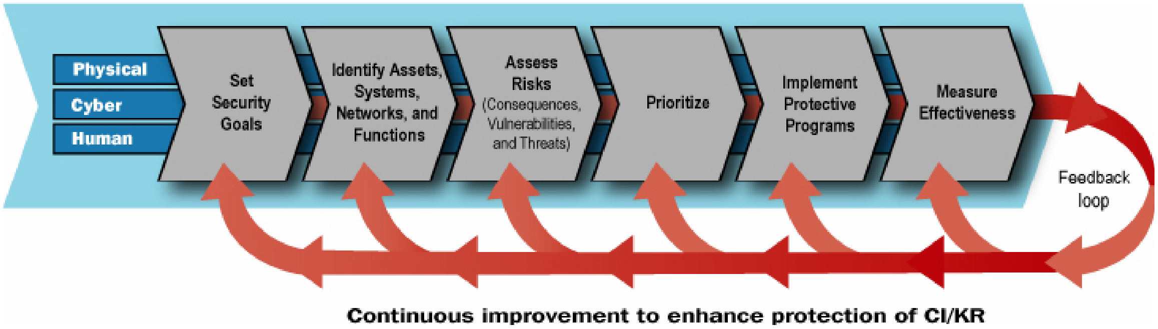
The NIPP identifies an overarching goal:

> *Build a safer, more secure, and more resilient America by enhancing protection of the Nation's CI/KR to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency.*

This goal also includes a risk management framework to support it. This risk management framework allows risk-reduction and protection measures to be applied where they offer the most benefit. Once security goals are set, the NIPP framework involves five subsequent key steps: (1) identifying CI/KR assets across the 17 sectors; (2) identifying and assessing risks; (3) normalizing, analyzing, and prioritizing study results; (4) implementing protective programs; and (5) measuring effectiveness.

Figure 1-2 shows the risk management framework outlined in the NIPP for developing each sector's security program. The expected output of this process is a set of sector-specific strategies to protect assets and systems. The Transportation Systems SSP builds directly upon this model, using it as the basis for its organization and as a starting point for its Systems-Based Risk Management (SBRM) approach.

Figure 1-2: NIPP Risk Management Framework


Physical
Cyber
Human
Set Security Goals
Identify Assets, Systems, Networks, and Functions
Assess Risks (Consequences, Vulnerabilities, and Threats)
Prioritize
Implement Protective Programs
Measure Effectiveness
Feedback loop
Continuous improvement to enhance protection of CI/KR

The Transportation Systems Sector recognizes the value of the NIPP framework for Federal, State, local, tribal, and private participants and is aware that each mode has unique characteristics, business models, system and asset classes, and sub-modes. Also, the sector members understand they must work together to achieve a consistent, sustainable, effective, and measurable security posture that preserves public safety and efficient commerce with minimal restriction of movement to cargo and people.

1.4.2 Systems-Based Risk Management Framework

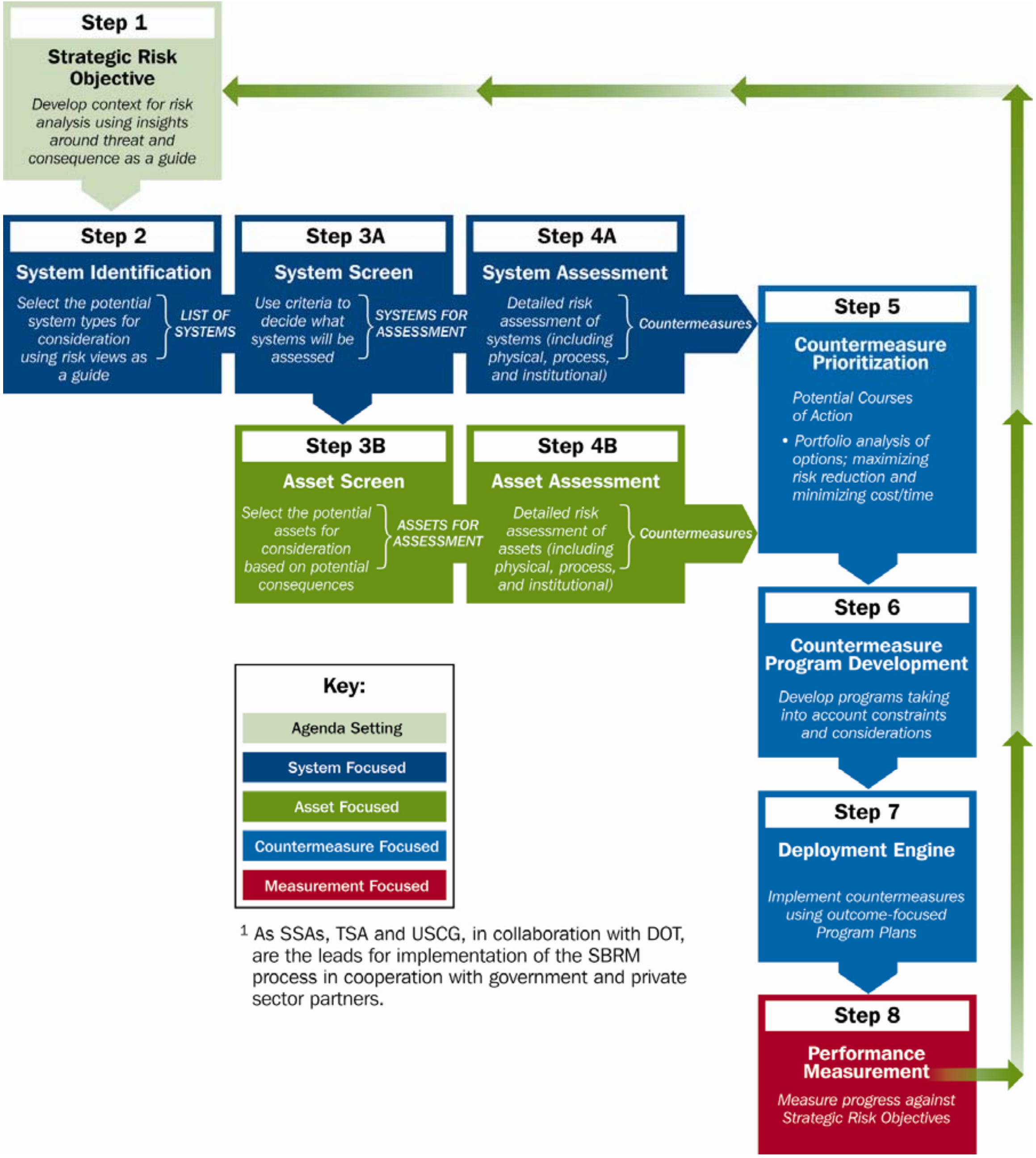
To achieve the security posture described in the previous section, the Transportation Systems Sector developed a collaborative methodology that applies a systems-based approach to managing threats, vulnerabilities, and consequences across the physical and cyber domains. As the agency responsible for managing strategic risks across the National Transportation System (NTS), TSA, as the SSA, not only looks at asset-level risk, but system-level risk as well. An asset-level risk is the combination of threat, vulnerability, and consequences for individual assets. System-level risks are those risks associated with combinations of assets, their relationships, their functions, and their emergent properties and characteristics. Because individual assets are part of a larger interconnected system, the consequences of a system-level failure can far exceed the consequences associated with a single asset. The SBRM approach accounts for network vulnerabilities and potential ripple effects—conditions created because of the interconnectedness and interdependence of transportation assets, systems, and functions nationwide—and augments asset-based risk assessments by providing insight into how the loss of individual assets or a collection of assets will impact the overall transportation system. This approach will enable the sector to better determine critical transportation systems and assets, and prioritize these systems and assets against limited resources (this approach is discussed further in section 3, Assess Risks).

The SBRM, shown in figure 1-3, links strategic goals and resulting performance to help meet the objectives as stated in this document and the NIPP. The SBRM process sets a strategic course for sector-wide risk management, yields strategic countermeasures, and does not specifically address operational or tactical planning.

The ability to manage risk by providing an integrated, structured, repeatable, adaptable process allows the Transportation Systems Sector to improve its risk management process over time. This process does not replace current methodologies and practices. Rather, it is an inclusive framework designed to use current processes and enrich the analysis of risk via a systems view.

Figure 1-3 illustrates the SBRM process that results in a comprehensive view of strategic risks in the transportation network. This risk management approach will identify specific strategic risk objectives (SROs) that will focus the development of a portfolio of asset- and systems-based risk management options. SROs, developed by both public and private industry leaders, are statements that establish a specific, measurable, realistic, attainable target that, when achieved, will improve the sector's risk profile. They set the target for required performance in light of specific consequences that span multiple stakeholders, transportation systems, or critical infrastructure sectors. Consequences can have nationwide implications to national security, health and human safety, the economy, the environment, or public confidence. To understand the evolution of those SROs and the sector goals that support them, which are laid out in section 1.5, the process that developed those SROs and the SBRM process that will update them in future iterations must be described.

Figure 1-3: Summary of Systems-Based Risk Management Process[6]

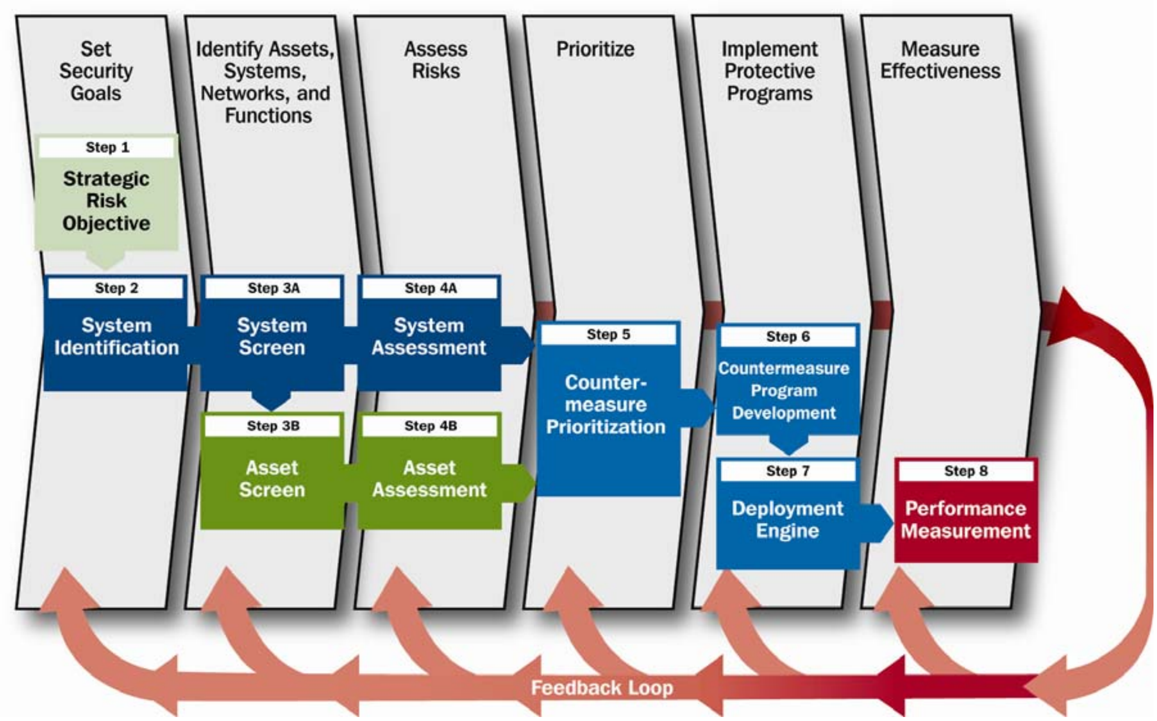

Step 1
Strategic Risk Objective
Develop context for risk analysis using insights around threat and consequence as a guide
Step 2
System Identification
Select the potential system types for consideration using risk views as a guide
LIST OF SYSTEMS
Step 3A
System Screen
Use criteria to decide what systems will be assessed
SYSTEMS FOR ASSESSMENT
Step 4A
System Assessment
Detailed risk assessment of systems (including physical, process, and institutional)
Countermeasures
Step 3B
Asset Screen
Select the potential assets for consideration based on potential consequences
ASSETS FOR ASSESSMENT
Step 4B
Asset Assessment
Detailed risk assessment of assets (including physical, process, and institutional)
Countermeasures
Step 5
Countermeasure Prioritization
Potential Courses of Action
• Portfolio analysis of options; maximizing risk reduction and minimizing cost/time
Step 6
Countermeasure Program Development
Develop programs taking into account constraints and considerations
Step 7
Deployment Engine
Implement countermeasures using outcome-focused Program Plans
Step 8
Performance Measurement
Measure progress against Strategic Risk Objectives
Key:
Agenda Setting
System Focused
Asset Focused
Countermeasure Focused
Measurement Focused
1 As SSAs, TSA and USCG, in collaboration with DOT, are the leads for implementation of the SBRM process in cooperation with government and private sector partners.

As shown above and explained in further detail in sections 3, 4, and 5, this plan seeks to ensure that the Transportation Systems Sector has the key capabilities required to manage strategic risks by building upon and extending current asset-based approaches. The SBRM process is an expansion of the six steps of the NIPP risk management framework detailed in figure 1-2. It focuses on three distinct areas: what we are concerned with (SROs), how the risk is understood using analytical evaluations, and how to manage risk by determining which countermeasures to invest in and

[6] As SSAs, TSA and USCG, in collaboration with DOT, are the leads for implementation of the SBRM process in cooperation with government and private sector partners.

measure. Figure 1-4 shows the relationship between the NIPP risk management framework and the Transportation Systems Sector's SBRM process.

Figure 1-4: NIPP Risk Management Framework/Systems-Based Risk Management Process



1.5 Transportation Systems Sector Security Goals and Objectives

The sector's security goals and objectives provided below are consistent with the goals outlined in the President's National Strategy for Homeland Security and the joint DHS and DOT National Strategy for Transportation Security (NSTS). These goals and objectives represent the initial view of the sector's security partners regarding strategic approaches for managing sector risk and include a range of flexible, layered, and unpredictable security programs that address the sector's risk-based priorities. The goals are supported by more specific and measurable objectives that indicate sector security priorities.

Initially, the sector vision statement, goals, and objectives were developed by the SSAs (TSA and USCG) and their Federal security partners (e.g., DOT, the DHS Office of Grants and Training (G&T), Customs and Border Protection (CBP), other agencies within the DHS, the Department of Defense (DOD), and the Department of Justice (DOJ)), drawing from existing national transportation security plans and strategies. From this initial effort, the Transportation Systems Sector modal Government Coordinating Councils (GCCs) and Sector Coordinating Councils (SCCs) provided vital comments and suggestions that enabled completion of the sector vision statement, as well as a set of goals and objectives.

The vision statement sets the stage for developing sector-specific security goals that are aligned with national goals. These strategic sector goals are needed to accomplish the sector's mission, as described below. Each stated goal is supported by a set of descriptive objectives.

Vision

Our vision is a secure and resilient transportation network, enabling legitimate travelers and goods to move without undue fear of harm or significant disruption of commerce and civil liberties.

Mission

Continuously improve the risk profile of the national transportation system

The Transportation Systems Sector's mission, to continuously improve the risk posture of the national transportation system, is the foundation of the risk framework. The future development of the sector's goals and objectives will be informed by the SBRM process and driven by the formulation of SROs through the GCC/SCC framework.

Goal 1: Prevent and deter acts of terrorism using or against the transportation system.

> *Terrorist attacks may seek to directly disrupt transportation systems or they may use transportation systems to carry out larger attacks against the American people. The primary goal of the Transportation Systems Sector is to prevent and deter criminal and terrorist attacks before they happen without disrupting the free flow of commerce or compromising civil liberties.*

Objectives

- Implement flexible, layered, and effective security programs using risk management principles. (Security measures need to be developed and established on the basis of risk analyses and should provide multiple opportunities to prevent an attack; should also continually evolve, introducing elements of uncertainty and unpredictability into an adversary's planning and surveillance efforts; and should be adaptable to different modes and threats in order to increase their robustness in the face of a dynamic and learning enemy.)
- Increase vigilance of travelers and transportation workers. (By having an active role in identifying and reporting suspicious activity, the traveling public and transportation workers can serve as force multipliers to Federal, State, and local law enforcement efforts.)
- Enhance information and intelligence sharing among Transportation Systems Sector security partners. (The development of relationships and improved technology can provide Federal, State, local, tribal, private sector, and international transportation security partners with a platform to share and exchange security information, such as threats, best practices, lessons learned, or other experiences to improve transportation security.)

Goal 2: Enhance resilience of the U.S. transportation system.

> *The resilience of a transportation system can be improved by increasing its ability to accommodate and absorb damage from natural disasters or terrorist attacks without catastrophic failure. Resilience-improving strategies include a wide variety of mitigation activities, including response and recovery activities.*

Objectives

- Manage and reduce the risk associated with key nodes, links, and flows within critical transportation systems to improve overall network survivability. (Many transportation systems contain a small number of critical assets that, if attacked, could result in catastrophic failure. These assets can take the form of a node, a link, or a flow. Security strategies must be identified to shift the threat away from these critical assets via risk management. The preferred risk management technique is to reduce risk; although, in certain cases, hedging, transferring, or even accepting the risk may be acceptable and warranted. If it is desired to reduce the risk, various approaches could be used, including deterrence and vulnerability reduction measures (as identified in Goal 1), or consequence mitigation measures, including hardening and increasing the redundancy of the key assets.)

- Enhance the capacity for rapid and flexible response and recovery to all-hazards events. (Response and recovery activities traditionally include first-responder actions and the plans, training, and exercises that support them. Response and recovery activities can also include pre-establishing re-routing procedures, emergency suppliers, and evacuation processes.)

Goal 3: Improve the cost-effective use of resources for transportation security.

> *Minimizing unnecessary duplication of efforts, improving coordination, and aligning resources to the highest risks all help the Transportation Systems Sector improve the cost-effective use of resources.*

Objectives

- Align sector resources with the highest priority transportation security risks using both risk and economic analyses as decision criteria. (The Transportation Systems Sector will collectively define its highest risks and work together to ensure that resources are appropriately aligned against them.)
- Ensure robust sector participation in the development and implementation of public sector programs for CI/KR protection. (In order to ensure that Federal, State, local, and private sector efforts are harmonized, the Transportation Systems Sector will utilize the GCC/SCC framework to jointly develop and implement security programs.)
- Ensure coordination and enhance risk-based prioritization of Transportation Systems Sector security Research, Development, Test, and Evaluation (RDT&E) efforts. (There are various research and development (R&D) efforts throughout the Federal Government and private sector. To avoid unnecessary duplication of efforts and to spur collaborative efforts, the GCC and SCC structure will be used to coordinate these efforts.)
- Align risk analysis methodologies with NIPP Baseline Criteria for assessment methodologies. (The NIPP Baseline Criteria states that risk analysis methodologies should be credible, documented, transparent, reproducible, and accurate, and they should enable sector leaders to make sound, cost-effective security decisions.)

1.6 Value Proposition

The Transportation Systems SSP is valuable to the American people if it enables the responsible public and private officials—the sector's security partners—to implement programs and activities that create a secure and resilient transportation network as described in the sector's vision statement. The sector's security partners should recognize the Transportation Systems SSP as the blueprint for building the protective end-state, as expressed in the vision statement. With a common understanding of the transportation network and a common application of the sector's risk management process, the security partners can develop cogent recommendations for changes in public policy. To address TSA's mission, the commitment and participation of the sector's many diverse stakeholders is vital to prevent, protect against, respond to, and recover from potential terrorist attacks and other incidents. High levels of communication and coordinated action are required, often within very short periods of time.

Each year, the Federal executive agencies receive billions of dollars, in aggregate, for security programs, grants, and R&D of homeland security initiatives. These agencies must make programmatic decisions on distributing funds and make proposals for future appropriations. Active participation in the development and implementation of the Transportation Systems SSP, through the GCC/SCC framework, affords stakeholders the opportunity to contribute significantly to shaping the Federal Government's risk-based decisionmaking.

1.7 Security Partners

The term "security partners" as used in the NIPP refers to the entire landscape of participants in the infrastructure protection planning process and includes all levels of government (Federal, State, Territorial, local, and tribal), regional organizations, international partners, and private sector owners and operators. The Transportation Systems Sector partnership model[7] will facilitate effective coordination between government and the private sector. Through this partnership, all sector security partners have roles and responsibilities in developing a robust SSP that is representative of their interests.

1.7.1 The Transportation Systems Sector-Specific Agencies

TSA was assigned responsibility as the SSA for the Transportation Systems Sector. The USCG was designated the SSA for the Maritime mode. TSA and USCG have the responsibility to implement HSPD-7 through the NIPP Sector Partnership Model.

1.7.2 NIPP Sector Partnership Model for the Transportation Systems Sector

The DHS has the responsibility for developing a comprehensive national plan for securing CI/KR and for recommending "measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other agencies of the Federal Government and in cooperation with State and local government agencies and authorities, the private sector, and other entities." The NIPP calls for implementing a sector partnership model as the primary organizational structure for coordinating and implementing CI/KR efforts and activities. The sector partnership model encourages formation of SCCs and GCCs as security partners to support activities required to implement and sustain the national, as well as sector-specific, CI/KR protection efforts.

Government Coordinating Councils

The primary mission of the GCC is to facilitate the development of comprehensive sector-wide strategies that advance CIP. GCCs may identify gaps in plans, programs, policies, procedures, and strategies, and serve as the forum to work with the private sector to develop, implement, and update each SSP. The designated SSA chairs each GCC, and the DHS Assistant Secretary for Infrastructure

[7] The Sector Partnership Model is the primary organizational structure for coordinating CI/KR efforts and activities as described in the NIPP.

Protection is the co-chair. The GCC serves as a counterpart to the SCC for each CI/KR sector and is composed of Federal, State, and local governments, and tribal interests.

The Transportation Systems Sector GCC was formed in early 2006 with the mission "to coordinate transportation security strategies and activities with all its security partners and establish policies, guidelines, and standards, and to develop program metrics and performance criteria for all transportation modes." The Transportation Systems Sector GCC fosters communication across government agencies and between the government and private industry in support of the Nation's homeland security mission. The GCC acts as the counterpart to the private industry-led SCC for transportation to review and develop the sector-wide security programs necessary to protect the Nation's transportation system.

The Transportation Systems Sector GCC includes the following member agencies:

- Department of Homeland Security (TSA, USCG, Infrastructure Protection, and G&T);
- Department of Transportation (DOT);
- Department of Energy (DOE); and
- Department of Defense (DoD).

The Transportation Systems Sector GCC will expand its membership as necessary.

By mid-April 2006, each mode in the Transportation Systems Sector began to develop its own modal GCC structure under the Transportation Systems Sector GCC and began to discuss priorities for joint work with their counterpart SCC. TSA representatives from each mode within the sector chair the modal GCCs (with the exception of the Maritime GCC, which the USCG chairs). The modal GCC structure includes members from the Transportation Systems Sector GCC, as well as other Federal agencies such as DOJ and the Department of Commerce (DOC) to name a few.

Through the Transportation Systems Sector GCC framework, shown in figure 1-5, Federal Government agencies with transportation security responsibilities are engaged and collaborate with the Transportation Systems SCC to refine and finalize the sector goals, develop the Transportation Systems SSP, and develop a mode-specific implementation plan to achieve the sector's goals. The GCC, working with the SCC, will serve as the integration council to ensure that CI/KR protection activities are accomplished. This may include:

- Structure an effective SBRM approach to identify and prioritize countermeasures within the sector;

- Plan and implement response and recovery activities and communication following an incident or event;

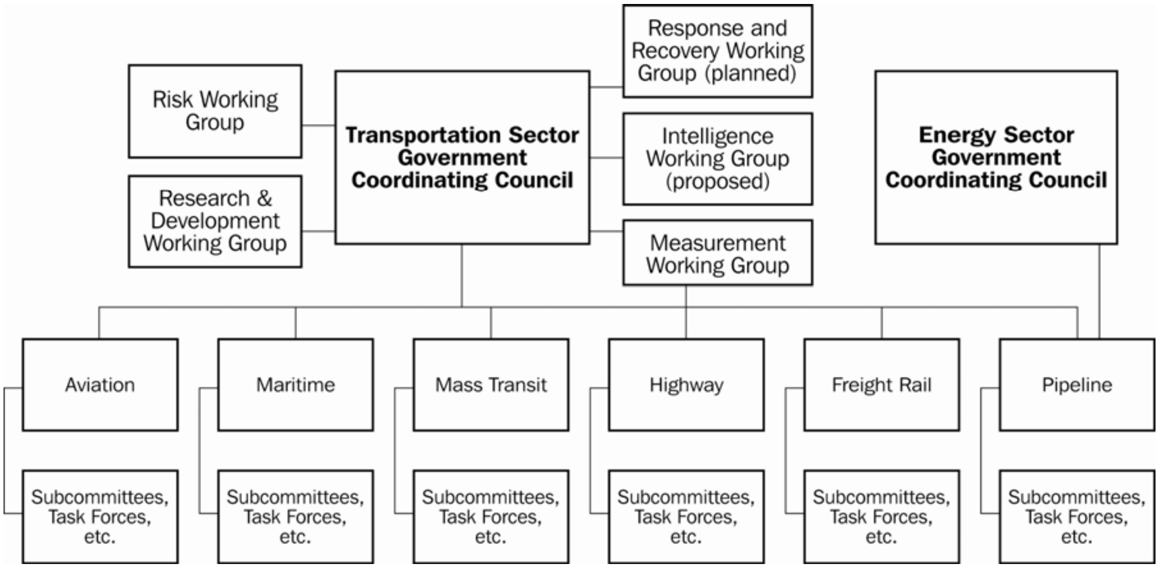
- Share credible intelligence and other relevant security information through communication mechanisms that are appropriate and effective;

- Facilitate the development of security guidelines, standards, regulations, and assessments;

- Identify and implement the information-sharing mechanisms; and

- Work with the SCC to enhance existing working groups and, when necessary, establish additional working groups.

Figure 1-5: Transportation Systems Sector GCC Organization

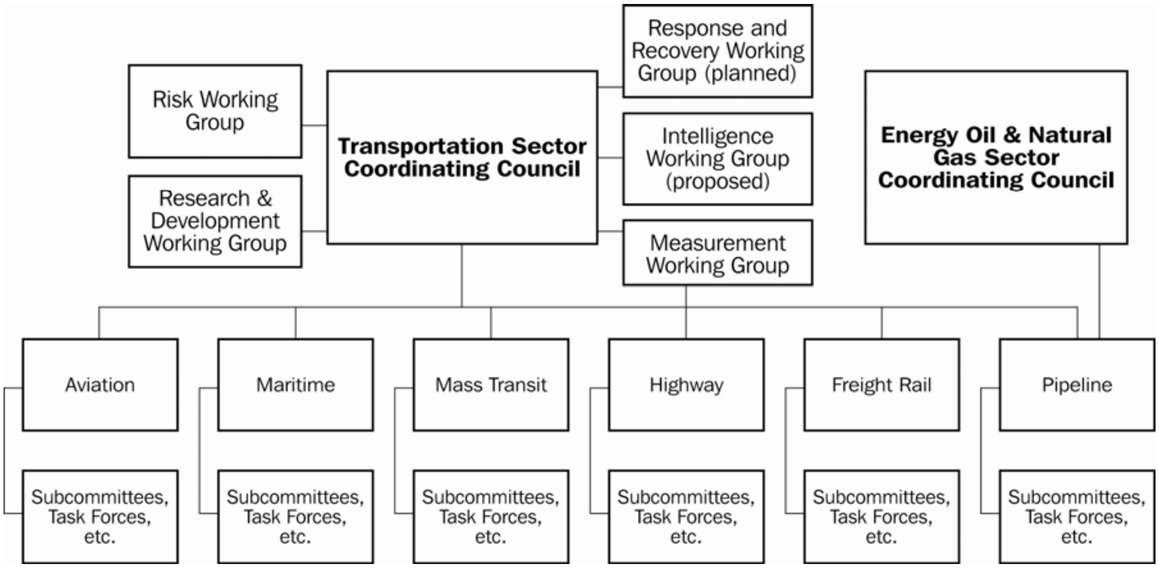

Response and Recovery Working Group (planned)
Risk Working Group
Transportation Sector Government Coordinating Council
Intelligence Working Group (proposed)
Energy Sector Government Coordinating Council
Research & Development Working Group
Measurement Working Group
Aviation
Maritime
Mass Transit
Highway
Freight Rail
Pipeline
Subcommittees, Task Forces, etc.
Subcommittees, Task Forces, etc.
Subcommittees, Task Forces, etc.
Subcommittees, Task Forces, etc.
Subcommittees, Task Forces, etc.
Subcommittees, Task Forces, etc.

Note: Refer to the Pipeline Modal Implementation Plan (annex F) for more information on the Pipeline GCC.

Sector Coordinating Councils

SCCs are self-formed councils composed of private sector representatives of infrastructure owners, operators, and related trade associations. Through the transportation SCC framework, private sector participants can provide input to the GCC to help refine and finalize the sector goals, develop the Transportation Systems SSP, and develop mode-specific implementation plans and programs to achieve the sector's goals. While the Transportation Systems SCC, shown in figure 1-6 below, is in the process of being organized, modal SCCs for each transportation mode have been established. Once the Transportation Systems SCC is organized and fully functional, membership can be expanded in the future, as necessary.

Figure 1-6: Transportation Systems SCC Organization


Response and Recovery Working Group (planned)
Risk Working Group
Transportation Sector Coordinating Council
Intelligence Working Group (proposed)
Energy Oil & Natural Gas Sector Coordinating Council
Research & Development Working Group
Measurement Working Group
Aviation
Maritime
Mass Transit
Highway
Freight Rail
Pipeline
Subcommittees, Task Forces, etc.
Subcommittees, Task Forces, etc.
Subcommittees, Task Forces, etc.
Subcommittees, Task Forces, etc.
Subcommittees, Task Forces, etc.
Subcommittees, Task Forces, etc.

Note: Refer to the Pipeline Modal Implementation Plan (annex F) for more information on the Pipeline SCC.

The SCC also plays an important role in providing expertise and leadership in CI/KR protection activities including, but not limited to:

- Contributing to an effective SBRM approach by working in partnership with the GCCs to identify and provide information regarding security measure priorities within the sector;
- Planning and implementing response and recovery activities and communication following an incident or event;
- Sharing information related to best practices, credible threats, risk data, incidents, domain awareness campaigns, etc.;
- Identifying and implementing the information-sharing mechanisms that are most appropriate for their mode (e.g., Homeland Security Information Network (HSIN), HOMEPORT); and
- Working with the GCC to enhance existing working groups and, when necessary, establish additional working groups.

Critical Infrastructure Partnership Advisory Council (CIPAC)

To secure our Nation's most critical infrastructure, the Federal Government and private sector must collaborate to identify, prioritize, and coordinate CI/KR protection, as well as share information about physical and cyber threats, vulnerabilities, incidents, and potential protective measures and best practices. To facilitate the successful execution of the sector partnership structure and to develop security plans, members of the SCCs and GCCs require an environment where they can discuss sensitive security matters. The DHS established CIPAC as an advisory council to the Secretary of Homeland Security under the provisions of the Homeland Security Act. CIPAC is exempt from the requirements of the Federal Advisory Committee Act (FACA). This is intended to enhance meaningful discussions between the Federal, State, and local governments, and the private sector on CIP issues. The process facilitates the sharing of security information and advice about sector strategies, protective programs and measures, threats, vulnerabilities, and best practices. GCC and SCC members must register to participate in CIPAC.

1.7.3 Key Federal Transportation Security Partners

Department of Homeland Security

The DHS's mission is to lead the unified national effort to secure America. The DHS will prevent and deter terrorist attacks and protect against and respond to threats and hazards to the Nation. The DHS will ensure safe and secure borders, welcome lawful immigrants and visitors, and promote the free flow of commerce. A number of offices and agencies within the DHS have responsibilities that directly or indirectly contribute to transportation network security. Additionally, agencies outside of the DHS also have responsibilities and interests in the Transportation Systems Sector.

The following are descriptions of Transportation Systems Sector GCC members.

- **Transportation Security Administration**. TSA was created under the Aviation and Transportation Security Act (ATSA), which gave TSA responsibility for security in all modes of transportation. As part of its security mission, TSA is responsible for assessing intelligence, enforcing security-related regulations and requirements, ensuring the adequacy of security measures at transportation facilities, and carrying out other transportation security responsibilities. Under HSPD-7, TSA was designated as the SSA for the Transportation Systems Sector by the Department of Homeland Security.
- **U.S. Coast Guard**. USCG is a multi-mission maritime service and one of the Nation's five Armed Services. Its mission is to protect the public, the environment, and U.S. economic interests in the Nation's ports and waterways, along the coast, on the high seas, or in any maritime region, as required, to support national security. In the event of a maritime incident, USCG will often act in a first-responder capacity. USCG also serves as the SSA for the Maritime transportation mode. The DHS, with USCG as its executive agent, has the primary responsibility for maritime homeland security, including coordinating mitigation measures to expedite the recovery of infrastructure and transportation systems in the maritime domain, with the exception of DOD installations.
- **Grants and Training**. The Office of Grants and Training is responsible for providing training; securing funds to purchase equipment; providing support for planning and execution exercises; and offering technical assistance and other support to assist States and local jurisdictions to prevent, respond to, and recover from acts of terrorism.
- **Office of Infrastructure Protection** (IP). The DHS IP has the overall responsibility for coordinating implementation of the NIPP across the 17 CI/KR sectors; overseeing the development of 17 CI/KR SSPs that outline processes and measures to secure the Nation's CI/KR; providing training and plans for protective measures to assist owners and operators in securing the CI/KR within their control; and helping State, local, tribal, and private sector partners develop the capabilities to mitigate vulnerabilities and identifiable risks to their assets. Through the NIPP Sector Partnership Model (SPM), the DHS IP coordinates security activities to reduce the Nation's vulnerability to terrorist attacks through a unified national approach.
- **Department of Transportation**. DOT has the responsibility for promoting safety, including hazardous materials security, through advocacy, regulation, enforcement, grants, and other means. DOT modal administrations manage many transportation programs that directly affect

the protection of critical transportation infrastructure. As stated in HSPD-7, DOT and the DHS will collaborate on all matters related to transportation security and transportation infrastructure protection in order to balance security requirements with the safety, mobility, and economic needs of the Nation and be prepared to respond to emergencies that affect the viability of the sector.

- **Department of Energy**. **As SSA for the Energy Sector, DOE is responsible for ensuring the security of the Nation's energy CI/KR. DOE is a member of the** Transportation Systems Sector GCC in its capacity as the lead Federal agency responsible for energy. Energy commodities are transported by pipelines, ships, barge, rail, and tanker trucks—assets and systems that cross over into the responsibility of the Transportation Systems Sector.
- **Department of Defense**. DOD is responsible for defending the Nation from external threats and owns a wide spectrum of support resources that could be requested during a transportation security incident. DOD has equities in the security of the commercial aspects of the Transportation Systems Sector and has policy devoted to the security of DOD shipments. DOD, as a member of the Transportation Systems Sector GCC, will be involved with the collaboration to determine transportation security policies and decisions. Agencies within DOD with transportation security responsibilities appear in appendix 4.

Additional Federal Security Partners

A number of Federal agencies work closely with the sector to ensure its security and the free flow of goods and passengers. Two agencies with direct involvement in transportation security are listed below. Other Federal security partners are listed in appendix 4.

- **Department of Justice**. DOJ acts to reduce criminal and terrorists threats, and investigates and prosecutes actual or attempted attacks on, sabotage of, or disruptions of CI/KR in collaboration with the DHS.
- **Federal Bureau of Investigation (FBI)**. The FBI is the principal investigative arm of the DOJ and the lead Federal agency for investigations of terrorist acts or terrorist threats by individuals or groups inside of the United States or directed at U.S. citizens or institutions abroad, where such acts are within the Federal criminal jurisdiction of the United States. Within the Transportation Systems Sector, the FBI will act to reduce terrorist threats, as well as investigate and prosecute actual or attempted terrorist attacks on, sabotage of, or disruption of CI/KR. The FBI will investigate and prosecute general criminal violations within the transportation system as directed by statute.
- **Customs and Border Protection**. CBP plays a key role in transportation security and protects against external threats that seek entry into the United States. CBP accomplishes this wide-ranging responsibility by reviewing and verifying cargo manifests, inspecting containers and persons, patrolling the Nation's land borders, and patrolling airways and marine ports. CBP officers are stationed at airports and seaports as well. CBP is also involved in security efforts pertaining to cross-border rail, trucking, and pipeline transportation.
- **Department of Commerce**. DOC has many component agencies involved with transportation security-related activities, such as the National Institute of Standards and Technology (NIST), the National Oceanic and Atmospheric Administration (NOAA), the National Telecommunications and Information Administration (NTIA), and the Bureau of Industry and Security (BIS). BIS advances U.S. national security, foreign policy, and economic interests for

DOC, and plays a critical role in the developing, promoting, and implementing policies that ensure a strong, technologically superior defense industrial base. BIS activities include regulating the export of sensitive goods and technologies in an effective and efficient manner; enforcing export control, anti-boycott, and public safety laws; cooperating with and assisting other countries on export control and strategic trade issues; assisting U.S. industry to comply with international arms control agreements; and monitoring the viability of the U.S. defense industrial base and seeking to ensure that it is capable of satisfying U.S. national and homeland security needs.

1.7.4 State and Local Security Partners

State and local agencies are often first on the scene of a transportation security incident. It is the responsibility of Federal officials to work closely with regional preparedness organizations to coordinate recovery efforts and restore public confidence following an attack. These agencies also work in close proximity to the owners or operators of the Nation's transportation infrastructure. Public safety agencies, such as law enforcement, fire/rescue, and emergency medical services (EMS) continue to be an integral part of gathering transportation security information and sharing it with the private sector owners and operators.

Additionally, the sector is working with the American Association of State Highway and Transportation Officials (AASHTO). AASHTO's Special Committee on Transportation Security (SCOTS) is responsible for advocating a secure transportation system by coordinating and collaborating with AASHTO members and other agencies and professional organizations. SCOTS membership includes three members (one voting member) from each member State. SCOTS has coordination interfaces with other AASHTO standing committees and subcommittees, such as the Standing Committees on Aviation, Highways, Public Transportation, Planning, Research, Rail Transportation, and Water, as well as subcommittees on Highways, Bridges and Structures, and Systems Operation and Management. In addition, AASHTO provides for security research through the Transportation Research Board (TRB) Cooperative Research Program.

1.7.5 Private Sector and Other Infrastructure Owners and Operators

Enhancing critical infrastructure security within the Transportation Systems Sector is a responsibility shared among all security partners—Federal, State, local, and tribal governments, as well as the private sector owners and operators. Since the private sector, as well as State and local entities, own and operate the majority of the transportation systems, a collaborative working partnership between the Federal Government and the private sector in fortifying all CI/KR security efforts and initiatives from their inception is essential. Therefore, the Federal Government must leverage industry's efforts in protecting critical assets through an effective public-private partnership. One manifestation of this partnership is mode-specific SCCs. A description of each modal SCC appears in its respective modal implementation plan annex.

1.7.6 International Organizations and Foreign Countries (International Activities)

The United States is an important trading partner with numerous foreign countries. Large volumes of merchandise enter the United States daily on ships and airplanes from across the world and by trucks and rail from multiple points along the Canadian and Mexican boarders. However, the September 11, 2002, attacks highlighted the security vulnerabilities now inherent in the global transportation network. The Transportation Systems Sector recognizes the need to engage with international partners to: (1) identify and understand threats, assess vulnerabilities, and determine potential impacts to the global transportation system; (2) exchange and share effective practices to deter, understand, and prevent future attacks; and (3) promote measures that safeguard the movement of people, goods, and services through international transportation systems.

It is vitally important that our global partners share critical information. This partnership will lead to more informed decisions by identifying and understanding threats, vulnerabilities, and consequences using global threat information and assessments. The Transportation Systems Sector (TSA, GCC and SCC members, etc.) must work together in order to improve and enhance security while maintaining an efficient flow of goods between international trading partners. Examples of this cooperation are the Security and Prosperity Partnership of North America (SPP), which establishes ongoing working groups, including representatives from various Federal agencies and Canadian and Mexican ministries to further North American security goals, and the International Maritime Organization (IMO), a specialized agency of the United Nations, which is responsible for measures to improve the safety and security of international shipping and to prevent marine pollution from ships. TSA has taken a leadership role in coordinating such relationships. Asia-Pacific Economic Cooperation (APEC) is the premier forum for facilitating economic growth, cooperation, trade, and investment in the Asia-Pacific region, and TSA played a key role in launching the Aviation Security Sub-Group in APEC.

Many security enhancement efforts are already underway; however, the Transportation Systems Sector, through the leadership of TSA, has identified several key strategic focus areas. These areas are: (1) assisting the International Civil Aviation Organization (ICAO) in the area of compliance and enforcement to ensure that aviation security vulnerabilities are identified through the Universal Security Audit Program; (2) increasing international focus on the need for pipeline, freight rail, and mass transit standards and/or best practices; (3) enhancing the ability of key international partners to identify terrorists and/or the instruments of terrorism by sharing technological expertise, lessons learned, and developing new advanced approaches; (4) strengthening international security baseline standards by actively participating in standard-setting organizations; (5) providing effective mechanisms for sharing and reporting information to foreign authorities and stakeholders through expert-level working groups, private conferences, bilateral meetings, and speeches; and (6) minimizing disruptions to the flow of passengers and commerce through regular consultations with international partners to discuss differences in policy or approach, working toward harmonization of measures.

Strengthening transportation security across all modes of the global transportation network requires strong collaboration worldwide to protect the traveling public from terrorism and reduces the potential for a disruption in the flow of commerce. The overarching goal is to strengthen transportation security practices by building and expanding partnerships with:

- The European Union (EU) (across all modes of transportation);
- European Civil Aviation Conference (ECAC);
- Asia-Pacific Economic Cooperation (across all modes);
- Civil aviation commissions in Latin America, Middle East, and Africa;
- The Group of 8 (the G8 is an international forum for the governments of Canada, France, Germany, Italy, Japan, Russia, the United Kingdom, and the United States) (across all modes);

- International Rail and Mass Transit Working Group;
- International Civil Aviation Organization;
- United Kingdom (Joint Contact Group, partnering at ICAO, and rail security);
- France (security cooperation and technical exchanges);
- Japan (technical exchanges and policy development, the 2006 Ministers of Transport Meeting in Tokyo, G8 coordination);
- Canada (pre-clearance, air cargo, Man-Portable Air Defense System (MANPADS), Smart Border, and SPP);
- Mexico (strengthening national-level oversight, MANPADS, ICAO audit preparation, and SPP); and
- Aruba, Bahamas, and Bermuda (aviation pre-clearance measures).

1.7.7 Other Advisory Councils

Aviation Security Advisory Committee (ASAC). ASAC's mission is to examine areas of civil aviation security as tasked by TSA with the aim of developing recommendations for improving civil aviation security methods, equipment, and procedures. The committee will provide advice and recommendations to the administrator for improving aviation security measures.

Homeland Security Advisory Council (HSAC). HSAC provides advice and recommendations to the Secretary of Homeland Security on matters related to homeland security. The council is comprised of leaders from State and local governments, first-responder communities, the private sector, and academia.

Marine Transportation System National Advisory Council (MTSNAC). Sponsored by the Maritime Administration (MARAD), the MTSNAC comprises 30 stakeholders throughout the MARAD Marine Transportation System (MTS) initiative. The council provides advice to the Secretary of Transportation on the state of the Nation's MTS and how it can meet the Nation's economic needs in 2020. The Security Committee of the Council works closely with USCG, TSA, CBP, and other stakeholders to address issues of cargo, port, and container security.

National Infrastructure Advisory Council (NIAC). NIAC is the President's principal advisory panel on CIP issues spanning all sectors. NIAC is composed of not more than 30 members, appointed by the President, who are selected from the private sector, academia, and State and local government, representing senior executive leadership expertise from the CI/KR areas as delineated in HSPD-7. NIAC provides the President, through the Secretary of Homeland Security, with advice on the security of physical and cyber critical infrastructure supporting important sectors of the economy. It also has the authority to provide advice directly to the heads of other departments that have shared responsibility for CIP, including DHHS, DOT, and DOE. NIAC is charged with improving the cooperation and partnership between the public and private sectors in securing critical infrastructure and advises on policies and strategies that range from risk assessment and management, to information sharing, protective strategies, and clarifying the roles and responsibilities between the public and private sectors.

National Maritime Security Advisory Committee (NMSAC). NMSAC will provide advice to the Secretary of Homeland Security via the Commandant of USCG on matters such as national security strategy and policy, actions required to meet current and future security threats, international cooperation on security issues, and the security concerns of the maritime transportation industry.

National Port Readiness Network (NPRN). NPRN is an organization of nine Federal agencies—DOT MARAD (chair), USCG, TSA, U.S. Army Corps of Engineers (USACE), U.S. Transportation Command (USTRANSCOM), U.S. Northern Command (USNORTHCOM), Military Sealift Command, Surface Deployment and Distribution Command, and U.S. Army Forces Command—with responsibilities for supporting the secure movement of military forces through U.S. ports. The organization includes a steering group, a working group, and local port readiness committees at 15 strategic commercial ports and provides coordination and cooperation to ensure the readiness of commercial ports and intermodal facilities to support deployment during contingencies and other defense emergencies.

National Institute of Standards and Technology (NIST). NIST is a non-regulatory Federal agency within DOC's Technology Administration. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. NIST, the only Federal agency with true metrology expertise (the only national metrology institute), has developed numerous homeland security-related minimum performance standards, participates (membership and committee chairmanships) in several standards setting bodies (American Society for Testing and Materials, National Fire Protection Association, International Association of Chiefs of Police, National Institute of Justice, Institute of Electrical and Electronics Engineers, Inc., etc.) related to homeland security, has extensive experience in designing and developing test and evaluation programs, provides nationally recognized accreditation of testing laboratories, and maintains memoranda of agreement (MOAs) with other nations regarding reciprocity of accreditation acceptance. The institute researches, studies, and advises agencies of information technology (IT) vulnerabilities and develops techniques for the cost-effective security and privacy of sensitive Federal systems. This is accomplished through the development of standards, metrics, tests, and validation programs, as well as establishing the minimum security requirements for Federal systems. NIST guidance aides in improving information systems security by raising awareness of IT risks, vulnerabilities, and protection requirements, and provides measures and metrics based on the guidance provided in a full risk management framework.

1.7.8 Academia, Research Centers, and Think Tanks

National Research Council, Transportation Research Board (TRB). TRB is one of six major divisions of the National Research Council of the National Academies. The board facilitates the sharing of information on transportation practices and policy by researchers and practitioners, providing expert advice on transportation policy and programs, including security and infrastructure protection policy and program development.

U.S. Coast Guard Research and Development Center. The center is the USCG's sole facility for performing RDT&E in support of USCG's homeland security and non-homeland security missions.

National Laboratories and Technology Centers. DOE's laboratories and technology centers house world-class facilities where more than 30,000 scientists and engineers perform cutting-edge research. The National Infrastructure Simulation and Analysis Center (NISAC), at Los Alamos National Laboratory, provides advanced modeling and simulation capabilities for analyzing critical infrastructures and their interdependencies, vulnerabilities, and complexities.

Homeland Security Centers of Excellence. Through the Homeland Security Centers of Excellence (HS-Centers) program, the DHS is investing in university-based partnerships to develop centers of multidisciplinary research where important fields of inquiry can be analyzed and best practices developed, debated, and shared. The DHS's HS-Centers bring together the Nation's best experts and focus its most talented researchers on a variety of threats that include those related to the transportation network.

Multidisciplinary Center for Earthquake Engineering Research (MCEER). MCEER, headquartered at the University of Buffalo, comprises a consortium of researchers and industry partners from numerous disciplines and institutions throughout the United States. MCEER's mission has expanded from its original focus on earthquake engineering to one that addresses the technical and socio-economic impacts of a variety of hazards, both natural and manmade, on critical infrastructure, facilities, and society.

The John A. Volpe National Transportation Systems Center (Volpe Center). DOT's Volpe Center in Cambridge, Massachusetts, is an internationally recognized center of transportation and logistics expertise. The center assists Federal, State, and local governments, and industry and academia in a number of areas, including human factors research; system design, implementation, and assessment; global tracking, strategic investment, and resource allocation; environmental preservation; and organizational effectiveness.

Homeland Security Institute (HSI). HSI's mission is to assist the DHS Science and Technology Directorate (S&T) and the DHS Operating Elements in addressing important homeland security issues, particularly those requiring scientific, technical, and analytical expertise.

2. Identify Assets, Systems, Networks, and Functions

2.1 Defining Information Parameters

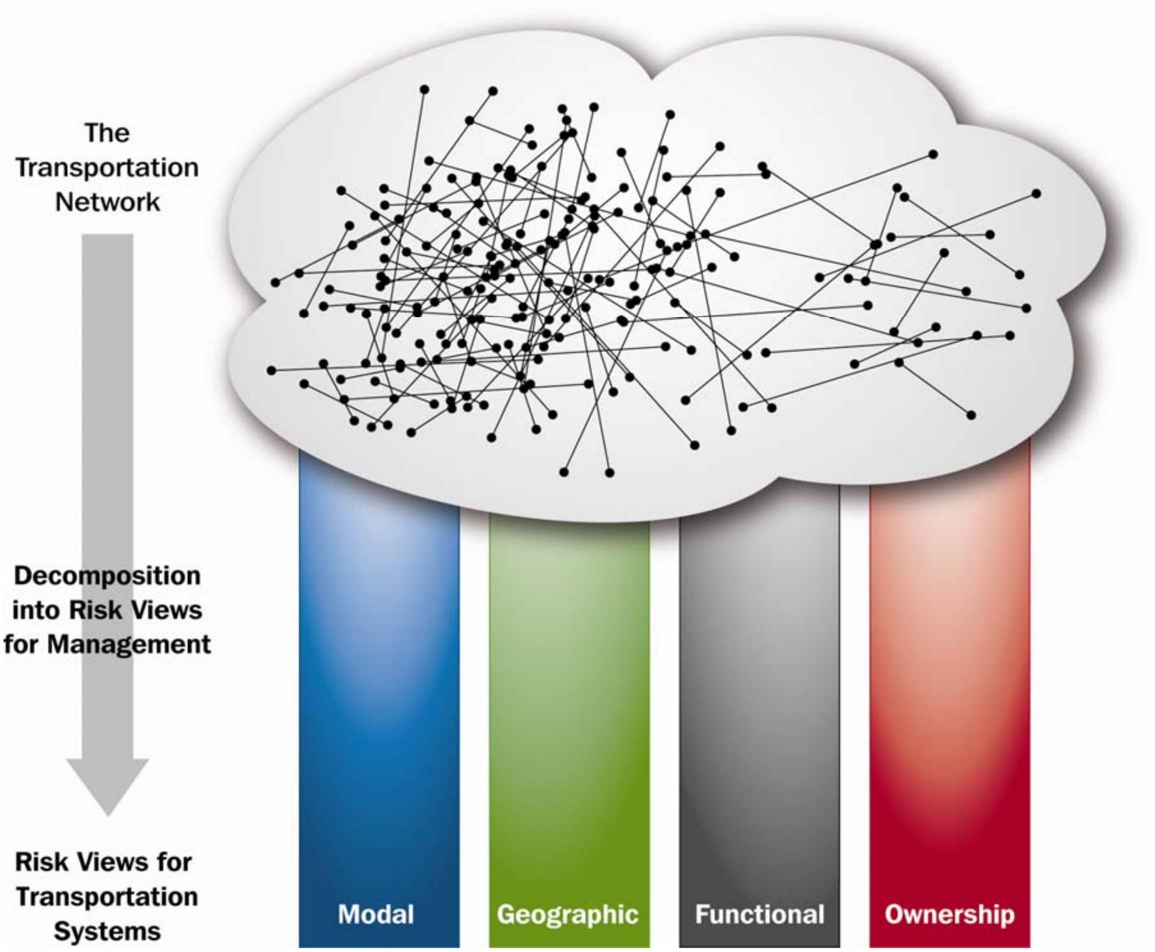
There are two complementary viewpoints from which the transportation network can be considered—a system perspective or an asset perspective. A system is a collection of transportation assets, their relationships, and their emergent properties that collectively come together to perform a function, supported by institutional rules and regulations, and structured around processes. Assets include a node, link, or flow in a transportation system and can be physical, cyber, or human in nature. See the goals in section 1 for a more detailed definition. In this section, the asset-based approach to collecting infrastructure information will be expanded. A systems-based consideration of the sector will also be further detailed. The following sections detail the information parameters associated with both systems and assets and how that information is collected, verified, updated, and protected.

2.1.1 Information Parameters for Systems

The national transportation network is a large, multifaceted, interdependent mix of links, nodes, flows, processes, agreements, rules, relationships, and regulations. This complex cloud of activity must be reduced into more manageable data to be used for risk analysis.

To assist stakeholders within the Transportation Systems Sector in defining systems, thematic perspectives or *risk views* will be used. Risk views, illustrated in figure 2-1, are distinct and complementary ways of evaluating transportation infrastructure and defining transportation systems. They are not mutually exclusive, nor is it presumed that the data collected in these views will be collectively exhaustive. Instead, the risk view structure supports a scalable system analysis capability, allowing for the examination of how risk manifests in the system. Risk views are the first step in defining the boundaries of a system, establishing relationships within the system, and identifying interdependencies. The initial set of risk views includes:

Figure 2-1: Risk Views Within the Transportation Systems Sector


The Transportation Network
Decomposition into Risk Views for Management
Risk Views for Transportation Systems
Modal
Geographic
Functional
Ownership

- **Modal**: Traditional industry delineation (i.e., Aviation, Maritime, Mass Transit, Highway, Freight Rail, Pipeline). All assets within a mode can be collectively evaluated as a system.
- **Geographic**: All assets within a geographic boundary (e.g., New York State or the city of Los Angeles). This view may be used most often by the G&T community, and State, local, and tribal government partners.
- **Functional**: All assets that, taken together, perform a specific function or service (e.g., supplying fuel to the Northeast). This view is supply chain-focused and may be used for example, by the USCG, CBP, interagency HAZMAT transportation working groups, and private sector partners.
- **Ownership**: All assets that fall under a defined set of decision rights, recognized by Federal, State, local, and tribal governments (e.g., all assets owned and operated by the New York Mass Transit Authority can be evaluated as a system).

2.1.2 Information Parameters for Assets

In working to protect the Nation's critical infrastructure, it is important that consistent terminology is used to facilitate communication and disseminate security information. Because the Transportation Systems Sector has a wide array of stakeholders, including commercial and industrial owner/operators and various Federal, State, and local agencies, it is important for the sector to adopt a taxonomy that will serve as the basis for how infrastructure is categorized within the National Asset Database (NADB).

The NADB is the Federal Government's repository for information on the evolving, comprehensive inventory of assets that comprise the Nation's infrastructure. The NADB taxonomy first groups CI/KR into the 17 broad sectors established in HSPD-7 and then categorizes them in more detail as needed. Up to five levels of detail are used, although not all infrastructure components require each level. Some infrastructure elements fall into more than one sector or have multiple components that fall into different categories of the taxonomy. In these cases, more than one sector or category is assigned to the piece of infrastructure. The SSAs (TSA and USCG), in addition to the DHS and DOT, have taken a comprehensive, integrated view of assets, including all characteristics and cross-sector CI/KR dependencies necessary for an asset to function. This integrated view is necessary because the functionalities of many assets depend on multiple elements and systems (e.g., people, electrical power, information technology (IT), or telecommunications). For the NADB transportation taxonomy, see appendix 5.

2.1.3 Information Parameters for Cyber Networks

The Transportation Systems Sector derives its understanding of critical cyber networks and assets from the USA PATRIOT Act; Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources; and HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection. The sector defines cyber networks as:

- An interconnected set of resources under the same direct management control (e.g., budgetary/operational authority for day-to-day operations and maintenance; system owners have the capability to effect changes in all areas that fall within the boundary of the system).
- An interconnected set of resources that have the same function or mission objective (entities within multiple systems that have identical/similar images and are geographically dispersed should be considered separate systems).
- An interconnected set of resources that have essentially the same characteristics and security needs (e.g., point of presence[8] defines a system; local area networks (LANs) and wide area networks (WANs) are different systems; persons under the Information System Security Officer (ISSO) manage security needs and administrative controls).
- A set of interconnected resources that reside in the same general operating environment (e.g., the ISSO must be able to see that operational controls are being enforced on day-to-day basis, attend to security incidents, and monitor/address security controls).

Collecting cyber data will be performed in the same manner as collecting data on physical transportation systems and assets.

2.2 Collecting Infrastructure Information

The collection of infrastructure information for the Transportation Systems Sector will cut across the four risk views (in addition to collecting asset-based data) to build a data set that is as comprehensive as possible. While this method may not be traditional in the way that owner/operators view their systems, it is reflective of the needs and responsibilities associated with

[8] A PoP (point of presence) is the location of an access point to the Internet.

the Federal perspective. One of the key advantages of constructing a data set from the four different perspectives on risk is that it builds a broad picture of the sector, which enables rich, system-based analyses. This also allows members of the sector to realize their place within the sector and understand how their system relates to others.

The ongoing effort to collect information will rely on data gathered from public and commercially available databases and from all Federal agencies and owner/operators who are requested to voluntarily submit CI/KR data on an as-needed basis. Existing statutory requirements can be a good source of infrastructure information; however, there are no standard collection requirements across the Transportation Systems Sector. Overall, the infrastructure identification process will continue to rely heavily on current processes and information sources. Where significant gaps exist, the sector will try to identify commercially available resources or request data from the owner/operator community. These data requests to the owner/operators will be voluntary, and those from the private sector will be encouraged to use the Protected Critical Infrastructure Information (PCII) Program when submitting information. The DHS is committed to protecting sensitive and confidential data from unintended disclosure using a variety of classification approaches in addition to PCII.

TSA is responsible for developing an understanding of data collection for asset dependencies, interdependencies, and critical functionality beyond what is required for the NADB, including collecting and storing system-level data. In conjunction with the GCC and the SCC members, the Transportation Systems Sector will work to identify targeted data sets, based on SROs, that are required to accomplish risk-informed security activities. While the NADB is currently asset-focused, the Transportation Systems Sector will seek to build a systems perspective into the existing NADB. This will not result in a secondary repository for information, but rather enhance the existing NADB.

In collecting cyber asset transportation data, TSA will use previous data collection efforts (e.g., the NADB); current TSA data collection approaches (e.g., Corporate Security Reviews, Risk Assessments, Rail Inspections, Commercial Site Vulnerability Checklist for Cyber Assets); and publicly available information, such as Securities and Exchange Commission filings. The GCC/SCC construct will serve as the primary vehicle for sharing cyber asset data within the sector. Cyber asset information will also be shared on an as-needed basis with other sector lead agencies, such as the National Cyber Security Division (NCSD) (Communications Sector) and the DOE.

Data gathered will be used in a variety of ways throughout the risk assessment and prioritization processes. Uses of the information will include, but are not limited to, risk assessments on systems, interdependency analyses, infrastructure modeling, infrastructure prioritization, and reporting. The Transportation Systems Sector will ensure that information protection mechanisms are in place to protect against misuse, unauthorized disclosure, or theft.

2.2.1 Data Collection Efforts—Systems

Collecting data through the systems risk view focuses on multiple, heterogeneous, geographically distributed systems that are embedded in networks at multiple levels. The four views capture multiple ways of addressing systems and add to a more robust assessment of the sector.

Modal View. The modal view treats all classes of assets within a mode collectively as a system. Infrastructure information in the modal view is categorized by interdependencies and supply chain implications that are specific to a particular mode of transportation. In addition to focusing on individual assets, nodes, and links, information specific to the modal view includes how those assets, nodes, and links interact within the mode and with other modes, their emergent properties and governing principles, or legislative information with specific modal impact. The sector will collect data through existing mode-specific data lists and readily available databases. Sector partners, in cooperation with other Federal agencies, State and local governments, the GCC and SCC, trade associations, nongovernmental organizations, and industry subject matter experts, will work to build a complete data set to best understand the risks to these modes.

Geographic View. The geographic risk view compiles transportation infrastructure data within specific regions of the Nation. The boundaries of those regions may vary based on the purpose and necessary parameters of an assessment. Regions may contain markedly different assets and systems, and thus the risks to those systems and the types of data collected from those regions will differ as well. Data collection in this view will allow an information set to be defined by what is physically located within that region and the processes or policies that impact that specific region. Therefore, assets, links, nodes, and emergent properties within a defined geographic area are evaluated as an integrated system.

Functional View. The functional view of data collection looks at the function a system fulfills within the supply chain. Examples of a functional view of systems include all of the assets, links, nodes, processes, policies, and emergent properties associated with:

- Delivery of critical medicines;
- Delivery of chlorine for drinking water or other purposes; and
- Delivery of heating oil to the Northeast.

By examining the function a system plays in society, the critical aspects of the system can be measured. This view also will have value in identifying interdependencies with other critical infrastructure. Collection efforts in the functional view are in the early stages and will be expanded over time.

Ownership View. The private sector owns approximately 85 percent of the Nation's assets. The ownership view examines information on ownership of assets, including the owner/operator's decision structure, policies, and procedures, and recognizes those assets owned by the same entity as an integrated system. Any data requested from owner/operators by the Federal Government for risk analysis need not be all-encompassing. Rather, infrastructure information required from owners by the Federal Government will be targeted and based on SROs.

2.2.2 Data Collection Efforts—Assets

Asset data is segmented by the six transportation modes. Data collection efforts by the Transportation Systems Sector will not attempt to be all-encompassing. In addition to using asset data collected in the NADB, the sector security partners will establish SROs through the SBRM approach, and only targeted data related to those SROs will need to be collected. The Transportation Systems Sector plans to employ the GCC/SCC framework to aid in the process of identifying and acquiring that targeted asset data. Specific information concerning the data collection efforts of individual modes can be found in the respective modal implementation plan annexes.

2.3 Verifying Infrastructure Information

Because of the complexity and size of the sector, sufficient resources do not exist to verify asset and system data for the entire sector. The Transportation Systems Sector will rely on stakeholders, including leading industry organizations and Federal, State, and local agencies, to help verify input. Federal infrastructure information compiled by other Federal agencies and used by the Transportation Systems Sector will be accepted as complete and not require immediate verification. For all risk views, multiple sources of information will allow cross-confirmation and the maintenance of a complete and up-to-date data set. Currently, a single methodology for verifying cyber asset information received from sector members outside of TSA has not been identified or employed. The SSAs will review currently available asset-specific information and group assets based on functionality and mode.

2.4 Updating Infrastructure Information

The SSAs intend to work with the DHS IP to expand the method for capturing systems information. Once asset and system information is verified, the sector will rely on sector stakeholders, including leading industry organizations and Federal, State, and local agencies, to help update and validate important infrastructure data. To improve stakeholder communications and expedite the flow of asset information, the Transportation Systems Sector will work across GCCs, SCCs, and Information Sharing and Analysis Centers (ISACs) to coordinate information updates.

2.5 Protecting Infrastructure Information

Information used and needed by the DHS and its security partners to effectively manage risk and secure the Nation's critical infrastructure often contains security information and/or sensitive business and proprietary information. As a result, information protection is paramount for those security partners who voluntarily supply critical information. The DHS has tools to protect security information by using the PCII Program. The program is managed by the DHS PCII Program Office within the Infrastructure Partnerships Division (IPD). The PCII program will protect proprietary and threat information from the private sector. The PCII Program will be administered by the National Infrastructure Coordination Center (NICC). The rules governing the PCII Program are located in Title 6, Part 29 of the Code of Federal Regulations (CFR). General information on the PCII Program is found on DHS's Web site at www.dhs.gov/pcii and in the NIPP base plan.[9]

Other regulations, in addition to the PCII Program, may affect the protection of data submitted to the DHS. For example, DOT and the DHS have regulations for protecting Sensitive Security Information (SSI) (49 CFR Parts 15 and1520). Information is protected as SSI if it meets the definition of any of the specific categories of SSI established in parts 15 and 1520, or that it otherwise must be protected from disclosure in order to ensure transportation security. Similarly, 46 United States Code (U.S.C.) 70103(d) (as implemented by 49 CFR Part 1520) requires that maritime security information, especially security assessments and plans, be protected from unauthorized access or disclosure.

[9] For more information, visit www.dhs.gov/dhspublic/display?theme=92 or www.dhs.gov/dhspublic/display?content=5476.

In addition to designating certain sector information as PCII or SSI, as appropriate, the Transportation Systems Sector must adhere to internal standards for protecting electronic information from a cyber attack. In a broad sense, TSA's compliance and oversight of the cyber security function is driven by goals set forth by legislation, regulations, policies, directives, and standards. In addition to OMB and the Federal Information Security Management Act (FISMA), the National Institute of Standards and Technology (NIST) was directed to produce numerous security documents. Because securing vulnerability assessment data is a central portion of the sector plan, TSA will use an integrated method to incorporate new security guidelines as they become available.

More information on the government's efforts to standardize and emphasize cyber security for all government facilities can be found in the Government Facilities SSP.

3. Assess Risks

3.1 Background

The Transportation Systems Sector faces a dynamic landscape of potential natural disasters, accidents, and terrorist attacks. To address the challenges posed by such risk, the sector will employ a comprehensive risk management program. Improving the overall risk profile of the sector will require an integrated asset- and system-based risk management approach. Asset-based risk management, essential to sector security, is widely practiced. However, transportation risk is not usually mitigated by "point" solutions alone (e.g., improving airport screening or erecting fences around a train station). Therefore, the sector will integrate asset-based risk management with a strong systems analysis designed to address the complexity of the transportation network. A systems perspective is needed to account for network vulnerabilities and potential ripple effects—conditions created because of the interconnectedness and interdependence of transportation assets, systems, and functions nationwide. Such a focus facilitates informed prioritization of decision options for securing critical assets, laying the foundation for a more effective and informed implementation of traditional asset-based approaches. The Transportation Systems Sector SBRM approach will identify and manage the sector's risk profile; develop standards and criteria for a common, relevant operational picture; and generate a portfolio of alternative management strategies that sector leaders can use to improve action and investment agendas.

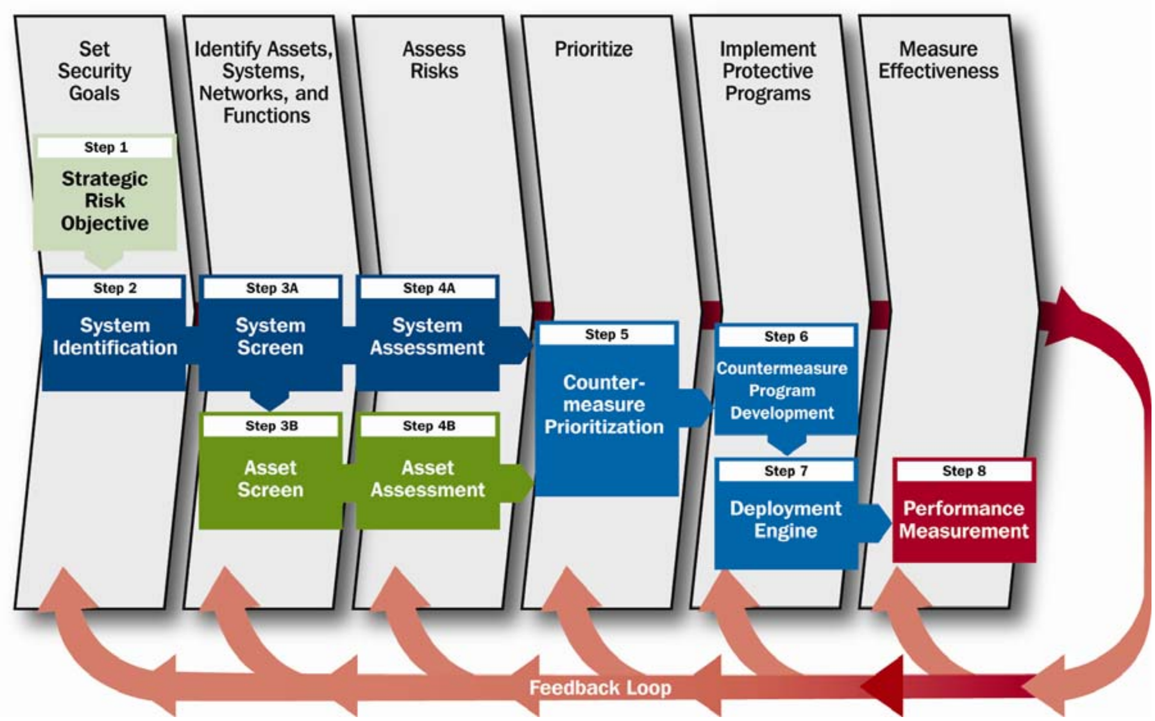
Consistent with Secretary of Homeland Security Michael Chertoff's vision for risk management, the Transportation Systems Sector's approach recognizes the important role that threat, vulnerability, and consequence play in the overall risk profile. Because of the difficulty in predicting terrorist threats, as well as the myriad vulnerabilities that exist in the transportation network, the sector is adopting a view of risk primarily driven by consequence. SROs will flow from an understanding of high-consequence risks to the network and will enable sector leaders to manage risk appropriately and effectively. Materiality, a blend of consequence and likelihood, will help to identify and prioritize SROs.

The approach described in this SSP is not the beginning of risk assessment for the sector, which has been ongoing for years and is crucial to transportation security; rather, it builds on existing programs to deliver an integrated systems-based approach. The SSAs will be responsible for coordinating this effort across the sector. Of course, risk management throughout the sector will be done in partnership with State, local, and tribal governments and with private sector owners and operators. Owners and operators assess their own assets and manage the risk to those assets, in some cases with assistance in various forms from the Federal Government. Information gathered through assessments and analyses enables the sector to consider which combination of countermeasures for assets, networks, systems, and functions will require risk management action and how those should be best applied at both the asset level and the systems level.

3.1.1 Relationship to the NIPP Guidance

To ensure the overall effectiveness of the Transportation Systems Sector's risk assessment methodology, the general approach described in the NIPP and the SSP guidance has been translated into a multi-step process—the SBRM methodology—that drives the development of mitigation options (e.g., risk management/countermeasure options). Each element of the NIPP guidance is addressed in the methodology, as shown in figure 3-1 below. While there are differences in terminology, the individual components of the SBRM approach directly relate to the objective of the NIPP risk management framework.

Figure 3-1: NIPP Risk Management Framework/Systems-Based Risk Management Process



3.2 Overview of the Transportation Systems Sector SBRM Methodology

The complexity and magnitude of the transportation network requires a robust and continuously informed risk management process. The SBRM methodology allows for sector-wide identification of and planning for those risks that, if realized, would have the most serious consequences for the transportation network. SBRM does not take the place of existing asset-based protection, nor is it intended as an operational or tactical plan. Instead, it takes a broader perspective and shifts the focus of the sector from specific point solutions to system-wide risk management. These perspective shifts are explained below.

3.2.1 Shifting From ASSETS to SYSTEMS

Asset-based data collection and risk assessment are underway across the sector and are an important component of transportation security. In the maritime mode, for example, the USCG's maritime security regulations at 33 CFR subchapter H that require facility and vessel security plans have generated information on thousands of maritime assets. The USCG continually reviews this information in its risk analysis. A systems-based approach examines how assets and systems interact with each other and the negative effects one could have on another if disrupted.

3.2.2 Shifting From REACTIVE to ADAPTIVE

Given increasing complexity and a constantly evolving threat environment, Transportation Systems Sector risk management must also be capable of adjustment and response to changing conditions.

Flexible security measures and improved information sharing greatly enhance the sector's ability to respond to changing threats.

3.2.3 Shifting From EVENTS to PATTERNS

Although a major consequence is a concern, it is the repetitive occurrence of terrorist attacks worldwide that will show patterns and, in recognizing those patterns, security measures can be identified.

3.2.4 Shifting From RIGID to RESILIENT

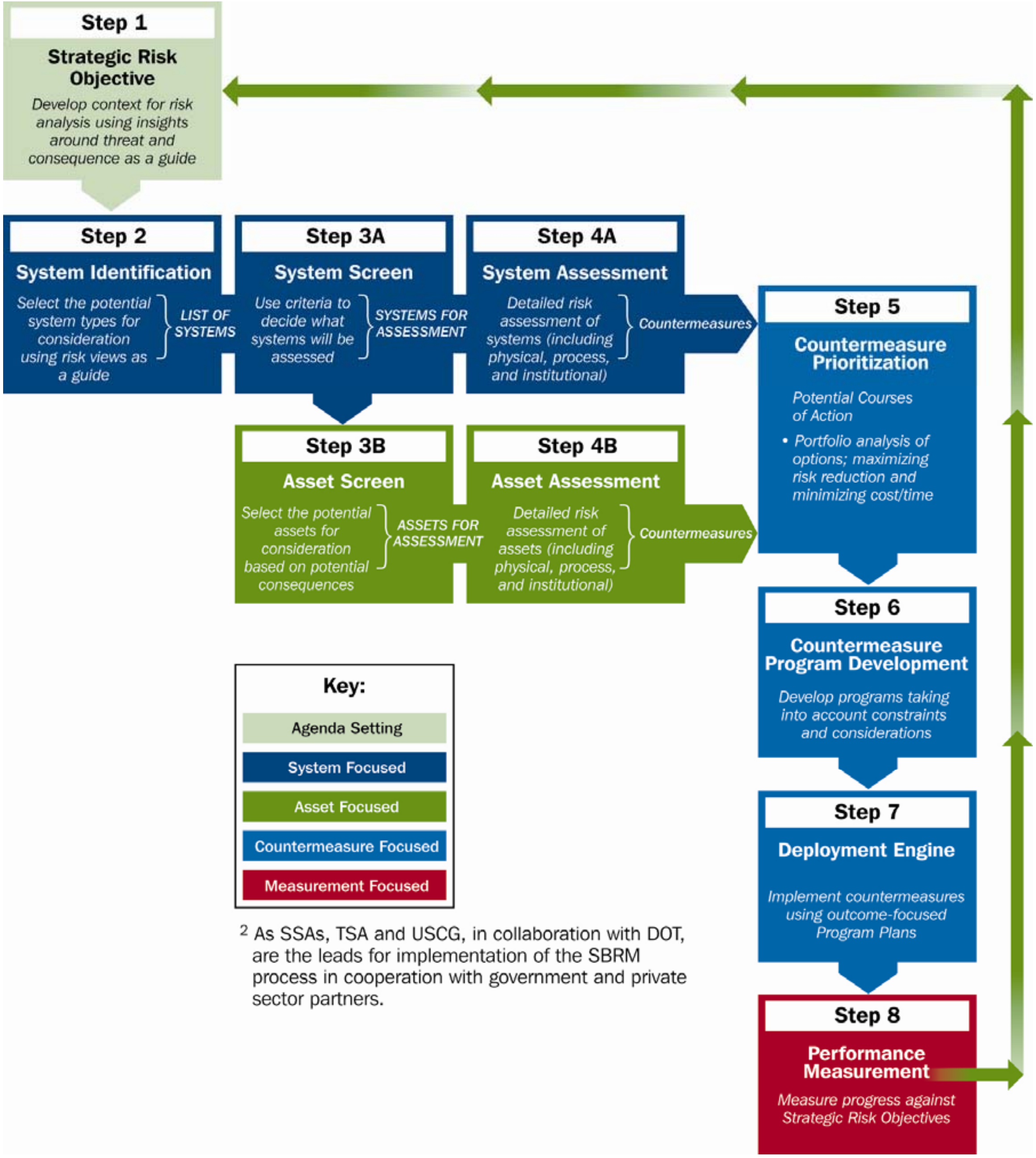
"Hardening" is an essential component of protecting critical assets and infrastructure. However, resilience of the transportation system can be improved by increasing its ability to accommodate and absorb unexpected shocks from natural disasters or terrorist attacks without catastrophic failure. Resilience-improving strategies include a wide variety of mitigation activities, including response and recovery activities.

The shifts in perspective allow the Transportation Systems Sector to view risk more accurately. By examining systems along with assets and focusing risk mitigation options on SROs likely to have the greatest impact on the network, resources can be more effectively allocated.

There are innumerable risks to the transportation network and an innumerable set of risk mitigation options. To meet the goal of continuously improving the risk profile of the transportation network with reasonable costs, the sector's varying stakeholders must focus and coordinate their respective efforts. To achieve such coordination, there must be focused and direct statements of intent from sector leadership. SBRM defines these statements as SROs. As previously stated, SROs, developed by both public and private industry leaders, are statements that establish a specific, measurable, realistic, attainable target that, when achieved, will improve the sector's risk profile. SROs are the driving force behind all risk-related decisions for the transportation network.

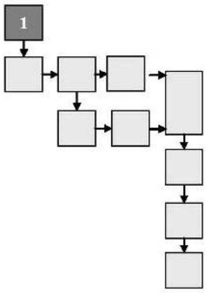
With clearly stated SROs as the planning guidance, the sector, as a whole, is able to identify systems and assets that require detailed risk assessments, prioritize countermeasure packages, develop countermeasure programs, implement effective programs, and monitor progress against objectives. As the methodology is inclusive of current ideas and tools, much of the ongoing risk-related activities performed by stakeholders fit within this framework. The following sections describe the steps of SBRM in detail, and figure 3-2 is highlighted to emphasize each step.

Figure 3-2: Systems-Based Risk Management Process[10]


Step 1
Strategic Risk Objective
Develop context for risk analysis using insights around threat and consequence as a guide
Step 2
System Identification
Select the potential system types for consideration using risk views as a guide
LIST OF SYSTEMS
Step 3A
System Screen
Use criteria to decide what systems will be assessed
SYSTEMS FOR ASSESSMENT
Step 4A
System Assessment
Detailed risk assessment of systems (including physical, process, and institutional)
Countermeasures
Step 3B
Asset Screen
Select the potential assets for consideration based on potential consequences
ASSETS FOR ASSESSMENT
Step 4B
Asset Assessment
Detailed risk assessment of assets (including physical, process, and institutional)
Countermeasures
Step 5
Countermeasure Prioritization
Potential Courses of Action
• Portfolio analysis of options; maximizing risk reduction and minimizing cost/time
Step 6
Countermeasure Program Development
Develop programs taking into account constraints and considerations
Step 7
Deployment Engine
Implement countermeasures using outcome-focused Program Plans
Step 8
Performance Measurement
Measure progress against Strategic Risk Objectives
Key:
Agenda Setting
System Focused
Asset Focused
Countermeasure Focused
Measurement Focused
2 As SSAs, TSA and USCG, in collaboration with DOT, are the leads for implementation of the SBRM process in cooperation with government and private sector partners.

[10] As SSAs, TSA and USCG, in collaboration with DOT, are the leads for implementation of the SBRM process in cooperation with government and private sector partners.

3.3 SBRM Step 1: Setting the Strategic Risk Objective



In order to make the process of risk management both tenable and effective, the GCC and SCC must focus on a specific set of objectives. As an initial step to establishing SROs, leaders from across the sector, specifically including private industry, will meet to discuss priority strategic risks. The intent of setting SROs is to enhance the current set of sector goals and objectives. Those SROs will be based on the materiality of certain consequences and the inability of the owner/operator community to address the priority risk without some form of Federal assistance. Full cooperation from the leaders of the sector, both public and private industry, is essential to establishing appropriate, realistic SROs. With consensus and cooperative efforts, the SROs will move from statements of intent to the motivating factors uniting sector-wide risk management efforts.

A defining characteristic of the sector's mission is that it is an ongoing activity—*continuously improving the risk posture of the national transportation system*—so the SROs cannot be static. Stated another way, an ongoing mission, like that of the Transportation Systems Sector, needs a constant stream of objectives inserted to ensure that the evaluation process is continuously utilized. The compilation of these objectives sets the direction for the management of strategic risk within the transportation system.

As discussed in section 1, each outcome-focused, sector-specific SRO developed will be supported by security measures designed to make measurable progress against the mission. Cross-cutting strategic goals will provide a framework to ensure that the sector deploys a balanced, comprehensive set of security measures to accomplish its SROs. In short, the SRO helps to clarify "what to focus on" based on the best available information. The strategic goals clarify "how to focus" based on public and private sector national priorities and lessons learned.

Once SROs have been identified, countermeasure programs that address those objectives will be coordinated within and across the security partners that compose the Transportation Systems Sector. In the interim, strategic goals outlined in section 1 have been developed to ensure progress against the mission.

The key to identifying a potential SRO is to capture it as an objective rather than a large-scale threat scenario. Table 3-1 shows the difference between the two concepts.

Table 3-1: Strategic Risk Objectives Compared to Threat Scenarios (Examples)

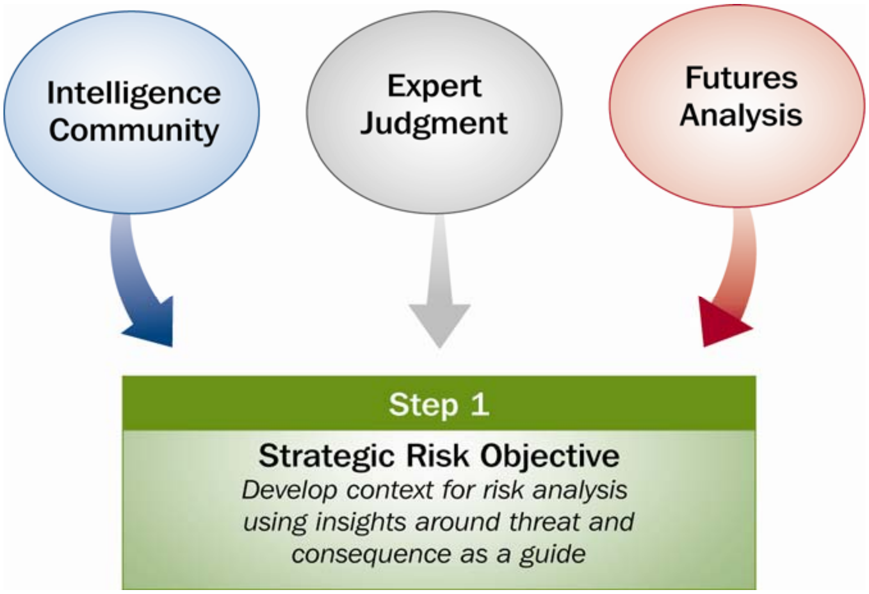
Strategic Risk Objective	Large-Scale Threat Scenario
Minimize the likelihood and impact of an attack on a major U.S. transit system.	Coordinated subway bombings
Prevent the destruction of U.S. aircraft by terrorists.	Improvised explosive device (IED) detonation during a flight
Minimize the likelihood and impact of an attack on a key, multi-modal transportation hub to the regional transportation system and to the national economy.	Release of bio-agent in a large airport
Minimize the likelihood and impact of an attack on an in-transit HAZMAT shipment on the U.S. transportation system.	Detonation of HAZMAT truck in a densely populated area
Minimize the likelihood and impact of a significant tunnel breach to the regional transportation system and to the national economy.	Tunnel breach and subsequent flooding of a city

3.3.1 Strategic Risk Objective Inputs

The process for determining SROs will be informed from three main sources: the intelligence community, expert judgment, and futures analysis. Each group will provide inputs based on its unique point of view. For example, the intelligence community may produce a fact-based review of current (classified) analyses to determine the most likely risks to the transportation network. The transportation industry professional community, including government and private sector stakeholders, will provide insight on the most likely risks to the system based on the intimate knowledge of existing transportation operations and the current security landscape. The futures analysis[11] group may use Red Cell or Alternative Futures review of current analyses to assemble and describe the most likely risks to the national transportation system based on their expertise. Each group's unique perspective is essential to formulating relevant and effective SROs.

[11] Futures analysis is a process in which an enterprise conducts long-term insightful research and analysis to better understand potential environment changes and identify the enduring strategies and capabilities necessary to achieve its mission in the future.

Figure 3-3: Inputs for Strategic Risk Objectives


Intelligence Community
Expert Judgment
Futures Analysis
Step 1
Strategic Risk Objective
Develop context for risk analysis using insights around threat and consequence as a guide

3.3.2 Consequence-Driven Strategic Risk Objectives

The SRO formulation process is grounded in an understanding of consequence. The sector's consequence assessment methodology considers a variety of factors, as discussed in the NIPP. The interconnected nature of sector risk is also key to determining consequence. Emphasizing consequence captures the difficulty associated with predicting terrorist threats; it also focuses on the overall effect of an attack—the potential human, economic, and psychological losses associated with terrorism. The following sets of questions exemplify consequence-based thinking:

- **Health and Human Safety**. What is the impact of a particular scenario on human life and physical well-being? For example, what levels of fatalities can be expected—either early or latent (e.g., as a result of diseases contracted or injuries sustained)?
- **Economy**. What is the impact of a particular scenario on national, State, and local economies? What are the expected costs of response and recovery? What is the expected cost of rebuilding assets or systems? To what extent will business operations and/or supply chains be disrupted and for how long?
- **Mission**. What is the impact of a particular scenario on the Federal Government's ability to maintain order, deliver essential public services, ensure public health and safety, and carry out national security-related missions?
- **Public Confidence**. What is the impact of a particular scenario on public morale and confidence in national economic and political institutions? If public confidence were to suffer, what would be the associated impacts on governance and the economy?

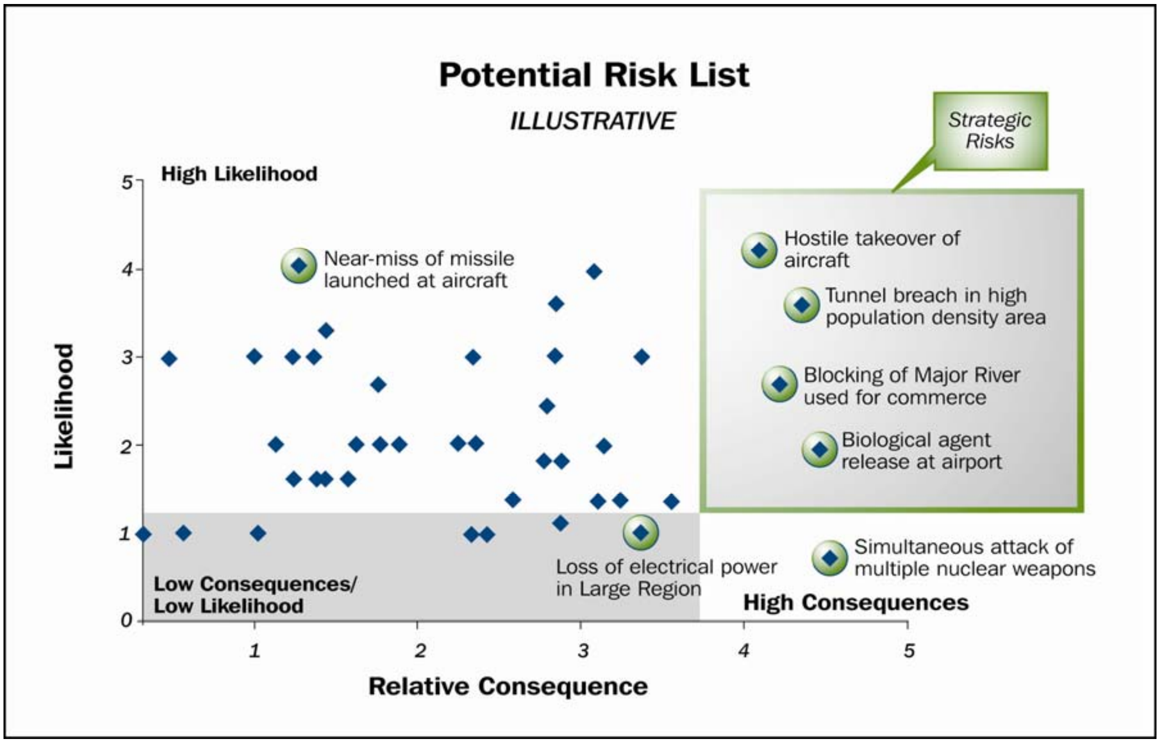
3.3.3 Materiality of Threats

For the sector's purposes, materiality is a function of likelihood and consequence for a given event. A threat is *material* if its manifestation could negatively and substantively affect the health and safety of the citizens, the national economy, the environment, public confidence, or the ability to conduct the business of governance.

An essential element of the consequence-driven risk management approach is the ability to address the escalating scale of consequence that comes about as a result of the "network effect." The term "network effect" refers to the exponential nature of systems, where every additional user increases the likelihood of even more users. Materiality depends on both the relative size of the impact and its likelihood of occurring. Since formulating SROs is fundamentally an expert judgment-driven process supported by information from the intelligence community, materiality provides a threshold or cut-off point to help defend and explain the selection of a given risk objective.

Figure 3-4 demonstrates how materiality can be used as a means of structuring the potential threats facing the transportation system. Each dot on the chart represents the combined likelihood and consequence of a threat.

Figure 3-4: Materiality Mapping of Potential Threats to the Transportation System



In the above figure, threats with a high relative consequence ranking and a high likelihood of occurrence represent greater materiality than those in the low/low quadrant. However, the other two quadrants still represent critical areas for consideration when assessing risk within a system. Each of the other quadrants has a "high" ranking in either consequence or likelihood, which means that each will be given consideration against the decision criteria.

Since the determination of materiality is a qualitative process, a variety of techniques will be used to extract the critical insights necessary to make this process transparent, traceable, and defensible. All these techniques will draw upon a wide array of technical and policy experts from across government, business, and academia in focused panels, interviews, and analytic sessions.

3.3.4 Assessing Threats

General Threat Environment. SROs will be formulated with a keen awareness of the various threats facing the sector. The chief threat is from terrorism. As the Brookings Institution noted, "from 1991 to 2001, 42 percent of all terrorist attacks worldwide have targeted rail systems or buses."[12] Terrorists understand that the open nature of the Transportation Systems Sector's infrastructure and operations are essential to the economic well-being of major cities or regions and numerous industries. However, terrorist attacks are only one of a number of potential threats that the sector faces. Natural disasters, as witnessed by the catastrophic Hurricane Katrina, and industrial accidents, such as the large HAZMAT spill on I-95 in Connecticut, also have serious economic, political, and psychological impacts on the sector.

To assist in creating an understanding of the general threat environment, the DHS, in coordination with the National Counterterrorism Center (NCTC) and the intelligence community, is preparing general threat environment documents for each sector. The documents, called Strategic Sector Assessments, can be used by industry, State, local, and tribal entities to assist in determining risk. Assessments will be prepared for each mode (Aviation, Maritime, Mass Transit, Highway, Freight Rail, and Pipeline).

While stakeholders have a legitimate need for current threat information to take immediate defensive action when appropriate, in the context of the sector's risk management approach, strategic threat analysis will be used to inform SROs.

Cyber Threats. Cyber threats to the Nation's critical infrastructure are addressed in unclassified documents such as the *National Strategy to Secure Cyberspace*, as well as classified reports. The cyber threat requires a substantial commitment from the public and private sectors to properly align resources, assess vulnerabilities, and protect critical networks from attack. America's critical infrastructure is under constant cyber attack; however, these attacks are varied and usually reflect criminal behavior rather than terrorism. The Transportation Systems Sector will work with the NCSD and affiliated analysts and experts in the intelligence community to monitor, assess, and respond accordingly to threats against the sector.

Process for Threat Analysis. Numerous intelligence agencies, such as NCTC, have specific roles in providing threat information to the sector. NCTC provides transportation security intelligence information to the Office of Intelligence (OI) within TSA to produce classified and non-classified annual threat assessments by mode and for the cargo/supply chain sector since 2004. These reports are disseminated throughout TSA, the DHS, and private industry. To produce accurate and comparable risk assessments, the formulation of assessments must be understandable, thorough, and repeatable. The sector recognizes the importance of private industry integration into the full intelligence cycle, consisting of private industry's intelligence requirements, tasking, analysis, and dissemination.

While the intelligence community provides numerous streams of raw intelligence to the DHS, USCG, and TSA, this information must be analyzed, filtered, and disseminated to sector stakeholders as classification and threat levels warrant. These communications are intended to solicit

[12] Arnold M. Howitt and Jonathan Makler, *On the Ground: Protecting America's Roads and Transit Against Terrorism*, The Brookings Institution Series on Transportation Reform, April 2005; see http://apps49.brookings.edu/dybdocroot/metro/pubs/20050426_howitt.pdf.

immediate action by stakeholders, especially private sector operation and tactical efforts. Modal GCCs and SCCs must work together to engage subject matter experts at the Surface Transportation ISAC, Public Transit ISAC, Highway ISAC, Maritime ISAC, ISAC Council, Association of American Railroads (AAR) Operations Center, and other information-sharing bodies to ensure the proper dissemination of intelligence. The sector will consider establishing a joint intelligence working group to better coordinate further integration. For long-term planning purposes, analyses will be packaged in a format and clearance level that enables sector stakeholders to understand threat in the context of a broader systems perspective, thereby facilitating input for developing SROs.

The roles and responsibilities of the various stakeholders in the threat analysis process are described below:

- **Transportation Security Administration, Office of Intelligence (OI)**: OI provides a capability to review, synthesize, and analyze transportation-specific intelligence. It is the only Federal entity focused solely on the security of the sector. OI intelligence products assist these critical TSA components in assessing risk and developing appropriate security programs, countermeasures, mitigation strategies, and protection guidance. The following is a list of the major OI threat assessment products (based on information received from NCTC and the intelligence community) that contribute to the sector's understanding of the terrorist threat:
- **Transportation Intelligence Gazette**: Concise written assessment of transportation-related intelligence, threats, and incidents. Produced frequently, as warranted, by intelligence reporting.
- **Threat Assessments**: In-depth written assessments of transportation-related intelligence and threat information.
- **Modal Threat Assessments**: Comprehensive threat assessments, produced annually at the classified and For Official Use Only (FOUO)/SSI levels, of the terrorist threat to each of the major transportation modes (Aviation, Maritime, Mass Transit, Highway, Freight Rail, and Pipeline) and to the cargo/supply chain sector.
- **Special Threat Assessments**: Written threat assessments of the transportation security implications of special events or dates of national significance (e.g., the State of the Union Address, the Super Bowl, and Independence Day) or international significance (e.g., the Olympics).
- **Weekly Field Intelligence Report**: Weekly compilation and analysis at the FOUO/SSI level of terrorist threats, trends, incidents, and suspicious events that are pertinent to transportation security personnel in the field. Based on intelligence, law enforcement, and open-source reporting.
- **Suspicious Incidents Report**: Weekly compilation and threat/statistical analysis of intelligence, law enforcement, and open-source reporting on transportation-related suspicious incidents.
- **Intelligence Notes**: Classified and FOUO/SSI assessments of transportation-related threat information; terrorist trends; terrorist incidents; and terrorist tactics, techniques, and procedures.
- **Transportation Situational Awareness Notes**: Written analysis/report of noteworthy transportation-related terrorist information, including threats; actual or attempted attacks; suspicious incidents; and tactics, techniques, and procedures.

- **United States Coast Guard, Intelligence Coordination Center (ICC)**: ICC provides all-source, tailored, and integrated intelligence and intelligence services to the DHS and its component agencies, such as TSA, the USCG Commandant and staff, the intelligence community, combatant commanders, and other services and agencies.
- **Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)**: HITRAC assesses intelligence information at a strategic level, looking not at individual targets, but at the transportation network on a larger scale. Modal analysts liaise with TSA analysts to produce coordinated intelligence analytic products. Transportation subject matter experts from various other agencies are also made available to HITRAC as requested.

3.3.5 Cross-Sector Information Sharing

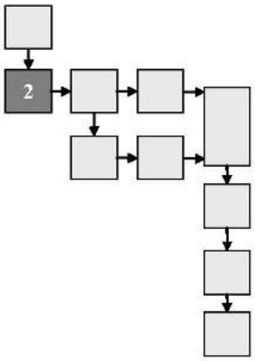
In the course of assessing and understanding threats to transportation infrastructure, communication among the sector stakeholders is vital to the overall security of the various systems. Many initiatives are already underway (discussed in section 8) and the sector will continue to support them.

As more risk data and analysis is available, ISACs and State and Local Fusion Centers (SLFCs) will become key players, helping to ensure that the necessary officials in the State, local, and tribal governments and the private sector are aware of their threat environment. TSA has piloted the deployment of Field Intelligence Officers to seven airports to directly support Federal Security Directors in their security duties, as well as build relationships with State and local stakeholders in the other modes.

DHS, TSA, and USCG analysts will continue to collaborate on numerous analytic products on threats to the sector and will work to disseminate assessments at the appropriate classifications to empower the greatest number of stakeholders with accurate and timely information. The Transportation Systems Sector GCC and modal GCCs will play central parts in building relationships with the sector stakeholders and in growing the trusted two-way exchange of information between private sector stakeholders and government risk management offices and leaders. This information-sharing effort is essential to meeting the priorities of the NIPP and the Transportation Systems SSP.

A feedback loop will also be established to ensure that insights gleaned from field assessments using specific threat input are shared with intelligence analysts throughout the intelligence community to continue to evolve their thinking and analysis. While State, local, tribal, and private sector needs for current threat information may still remain high, for the purposes of risk assessments, strategic threat objectives will be more applicable and useful to the sector in understanding its overall risk profile.

3.4 SBRM Step 2: System Identification

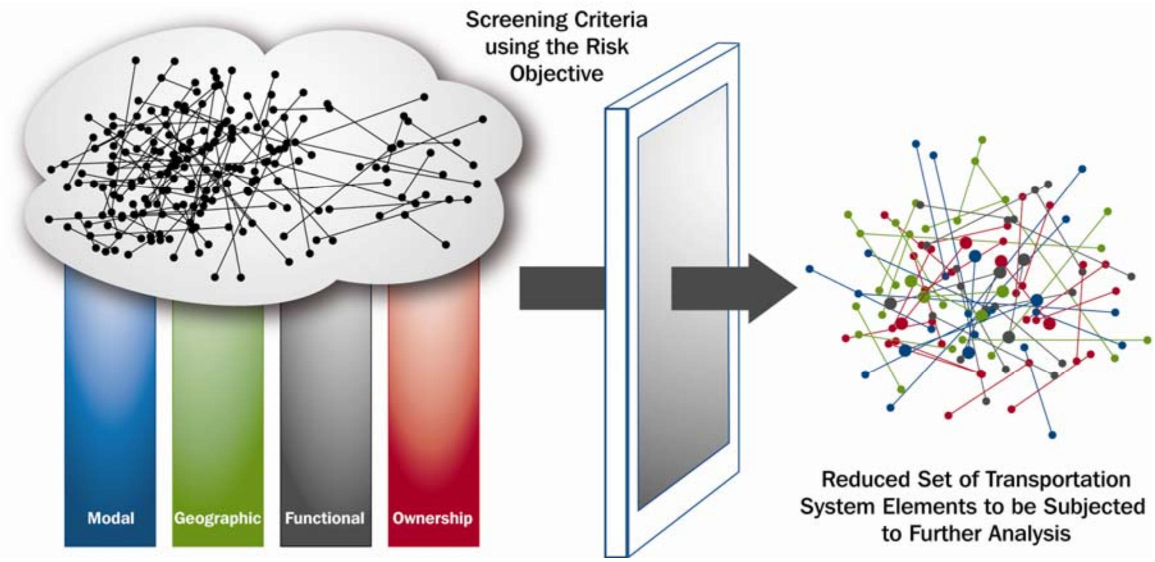


After an SRO is determined, the next step provides a formal review of the transportation network so that a feasible model can be developed and analyzed effectively. This step effectively reduces the “universe of options” by determining those transportation systems that have little to no impact on an SRO. For a risk objective such as “minimizing the downtime of large airports affected by a natural disaster,” there may be a clear set of systems that need not be considered (e.g., rail, maritime) because they are effectively outside the scope of the analysis. Other objectives, such as “improve the ability of the transportation system to withstand the impact of a Category IV or V hurricane,” will be more inclusive of modes and less inclusive of locations (geography). While an obvious initial step, identifying systems is crucial to the subsequent steps involving complex system and asset assessments.

3.4.1 Initial System Screening

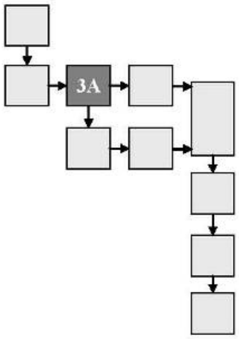
By using the different risk views—modal, geographic, functional, and ownership—as a guide, a more comprehensive list of systems will be generated. Effectively, this step reduces the universe of options by making a value judgment on transportation systems that have very little to do with a given objective. Figure 3-5 depicts the identification and filtering process.

Figure 3-5: Identification and Screening Process


Screening Criteria using the Risk Objective
Modal
Geographic
Functional
Ownership
Reduced Set of Transportation System Elements to be Subjected to Further Analysis

Following the application of each view to the transportation network, the resulting system is further characterized. The SBRM output for this step is a reduced set of systems of potential interest to be considered in the system screening process that is defensible and traceable.

3.5 SBRM Step 3A: System Screen



Following step 2, a refined view of the system is ready for analysis. Step 3A allows for further refinement of the system to be analyzed and develops a working model that can be used to simulate scenarios pertinent to the SRO. These activities are achieved in three primary substeps:

- Apply system screen;
- Define system operations; and
- Baseline system performance.

3.5.1 Apply System Screen

Even the reduced set of systems from step 2 is challenging to evaluate and draw any meaningful conclusion from in a reasonable timeframe. Step 3A further filters the systems of potential interest using operational performance goals (baseline requirements for system operation derived from the SRO) as the basis to determine which subsystems and elements will be subjected to a much more detailed analysis. This step is analytically necessary given the often inverse relationship of system size to the specificity of the countermeasure. The SBRM framework strives to capture the most specific and action-oriented countermeasures possible. To do this, analysts need to be working with as reasonably sized and issue focused a system as possible. Step 3A takes the systems determined to have a strong association with the SRO and selects from that set a reasonably-sized and issue-focused system, and then baselines its performance for further study.

3.5.2 Define Systems Operations

Upon further filtering of the transportation network, defined in step 2, relationships and connections within the network need to be modeled and understood. To achieve this, a suite of network modeling tools can be used. A key output of this step is that an accurate rendering of the system under study has been captured and stored.

Network Structure of Each System. Relationships within the transportation network need to be defined at two levels. The first is to understand key interdependencies and linkages between assets. This leads to a representation of the various parts of the system as a network, where nodes are represented as assets and links represent the physical connections between these assets or nodes. Physical information about the transportation system can be acquired through relevant industry data sets and through experts in this realm.

Additional layers of information also need to be captured regarding the institutions and processes governing the system. To properly capture this information, experts may need to be solicited again. While information on institutional processes and procedures may be harder to capture, unlike the physical system, the key relationships between the three layers need to be understood and documented prior to moving to the next substep. However, it is also important to note that a complete data set is not required to move into the next step of the process.

Intersystem Relationships. The previous substep defines, characterizes, and illustrates different components of the transportation network. Additional research is also needed to document the relationships between these various systems. Key relationships exist between separate transportation systems. For example, the rail and aviation systems share common assets (e.g., stations and airports) that are major hubs for both. These locations demonstrate an interrelationship between the systems and need to be documented.

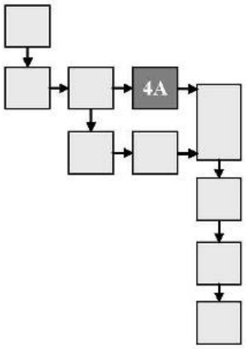
Each separate transportation mode needs to be reviewed to locate and document physical relationships with other systems. Additionally, the same effort is required for the institutional and process layers of each system. Through this effort, an accurate depiction of the current transportation network will be established and available for analysis in the context of the SRO.

3.5.3 Baseline System Performance

Creating a complete baseline model or configuration is a key product of step 3A. Simply stated, the baseline configuration will capture a "rendering of the system"—a depiction of how the system performs under normal conditions. Key to the SBRM's analytical approach, this configuration will enable the sector to understand the impact of specific scenarios (e.g., loss of assets or nodes) on system-wide performance and will facilitate the development of countermeasures in step 4A.

Expert judgment, historical data, and various analytical models will most likely provide baseline calculations. It is important to note that the breadth and comprehensiveness of baseline models will vary depending on the system under study and on the complexity of its associated layers. A complete model is not required to move into the ensuing system assessment step.

3.6 SBRM Step 4A: System Assessment



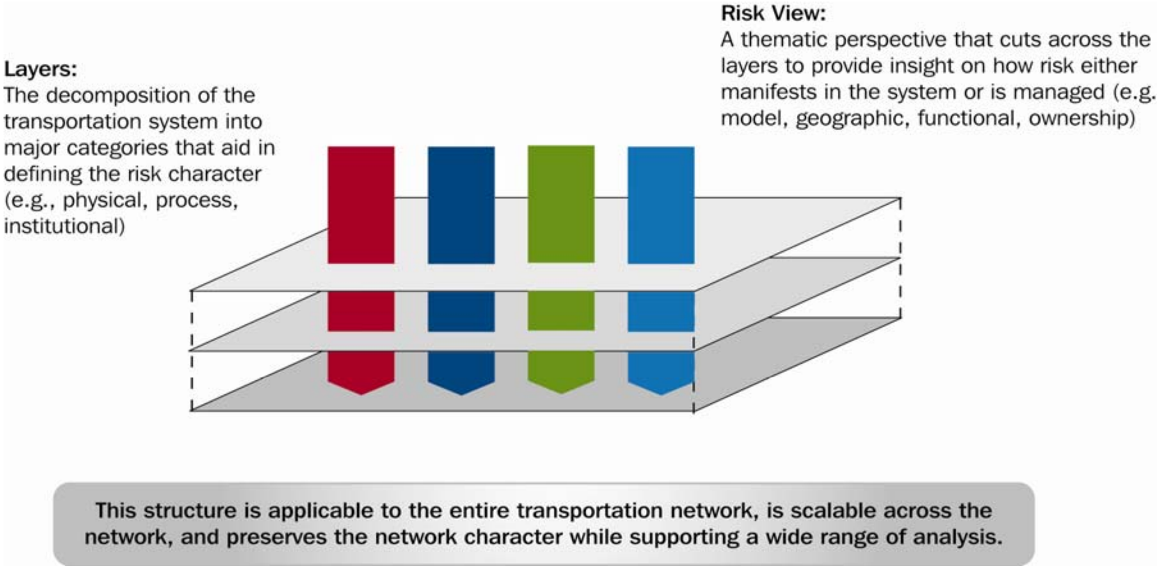
Assessments at the system level are a key component of the sector's SBRM methodology. These assessments assist in identifying and prioritizing risks for infrastructure owners and operators, as well as the government. The SBRM System Assessment identifies, models, and evaluates the effectiveness of countermeasures in targeting systemic vulnerabilities that help the sector achieve SROs. Step 4A involves three main substeps:

1. Analyze system performance and develop countermeasures at the system level;
2. Assess the effectiveness of countermeasures through countermeasure effectiveness modeling; and
3. Finalize a list of proposed system countermeasures.

3.6.1 Analyze Performance and Develop Countermeasures

Even with the informed filtering done in step 2, the baseline representation of the system of interest from step 3A contains a near infinite set of conditions that could be considered. The purpose of this substep is to focus the attention of the detailed analysis on the vulnerabilities (or, more accurately, the perceived weaknesses) in the system that would have the greatest potential impact relative to the SRO if exploited. Three risk layers—physical, process, and institutional—all add to overall system understanding and inform countermeasure options (see figure 3-6).

Figure 3-6: Risk Layers in the Transportation Systems Sector



Layers:
The decomposition of the transportation system into major categories that aid in defining the risk character (e.g., physical, process, institutional)

Risk View:
A thematic perspective that cuts across the layers to provide insight on how risk either manifests in the system or is managed (e.g. model, geographic, functional, ownership)

This structure is applicable to the entire transportation network, is scalable across the network, and preserves the network character while supporting a wide range of analysis.

- **Physical**. The physical level comprises the material components or assets necessary for the continuous operation of the transportation system. For example, the physical components of the rail system include stations, rail cars, tracks, and switches.
- **Process**. The process level comprises the rules, actions, and decisions that give life to the physical level and are necessary for efficient and effective operation of the transportation system on a daily basis. This level captures the ways in which assets work together—physically or virtually. In some cases, these systems may be physically distant from the action they direct. For example, again using the rail system, the process level includes how a particular railroad entity educates its employees and regulates their activity in relationship with established routing guidelines for moving between stations.
- **Institutional**. The institutional level comprises the policy and guidance that empower and constrain the operation of the transportation system to meet the large-scale public objectives essential to long-term sustainability. This includes Federal legislation, national policies, State regulations, and workforce policies. To complete the rail example, the Federal Railroad Administration (FRA) administers track safety standards that govern the building, usage, and maintenance of rail track. Additionally, USCG maritime security regulations, the National Strategy for Critical Infrastructure Protection, State Security Directives, and on-site training or security policies are all part of the institutional level.

A key element of this substep is to identify the primary focus of the system assessment (i.e., system vulnerabilities) and consider possible ways to counter them. Using system/network analysis techniques to assess the system-wide consequences, potential countermeasures are developed. These countermeasures are considered in the context of the SRO-specific analysis criteria and more generalized consequence criteria derived from the NIPP. In addition, this element examines system-wide threats and uses qualitative techniques to develop potential countermeasures to threats to the system.

3.6.2 Assess Effectiveness of Countermeasures

Countermeasure effectiveness modeling is conducted to see what impact the countermeasures have on the system and assists in making a determination of which countermeasures are worth pursing based on the positive effect on key performance measures.

Countermeasures are, of course, intended to enable the system to reach adequate performance measures, as outlined by the SRO. Therefore, potential countermeasures need to be evaluated in the context in which the system will operate—namely, a nonlinear and interdependent, multi-faceted threat environment. Moreover, many of the potential countermeasures will themselves depend on the ability to assess their value as it relates to managing systemic effects. All of this points to the need to perform consequence modeling using nonlinear analysis techniques and models. For example, this substep may use the following two modeling methods:

- **System Dynamic Modeling** is an approach to understanding the behavior of complex systems over time. It deals with internal feedback loops and time delays that affect the behavior of the entire system. What makes using System Dynamics different from other approaches to studying complex systems is the use of feedback loops and stocks and flows. These elements help to capture the nonlinearity of a system using the relationships of the components as the basis of the model.
- **Agent-Based Modeling** is a specific individual-based computational model for computer simulation extensively related to the theme in complex systems, emergence, Monte Carlo Method, computational sociology, multi-agent systems, and evolutionary programming.

These models could be used to assess how the complex systems perform under changes imposed by the countermeasures.

3.6.3 Finalize List of Proposed System Countermeasures

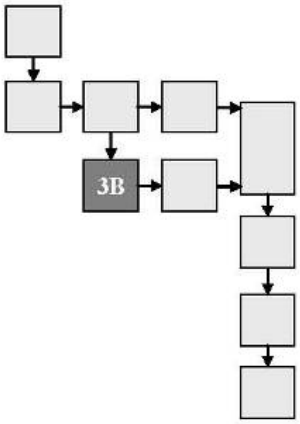
After determining the effectiveness of each proposed countermeasure and settling on the best candidates, the last substep of 4A is to assess countermeasure feasibility constraints and key considerations. This analysis will inform step 5 (prioritization) and step 6 (countermeasure program development) of the SBRM process. While the effectiveness is a key element in determining the sector's portfolio of countermeasures to accomplish SROs, additional factors must be considered. Likely constraints and considerations include:

- **Internal Government Cost**. How much would it cost Federal, State, and local governments to implement this countermeasure?
- **Cost to Industry.** What economic impact could implementing this countermeasure package have on transportation stakeholders?
- **Level of Confidence in Countermeasure**. How much does the projected countermeasure package's effectiveness depend on assumptions? What is the confidence level that the projection is accurate?
- **Likelihood of Success/Difficulty.** Is the package a long shot, but with a very high payoff if successful? Does the package have minimal impact, but is very easy to achieve?
- **Sector Capability**. Is the sector capable of executing the countermeasure package?

- **Time to Implement**. How long will it take to implement the countermeasure? How soon can the first countermeasure begin?
- **Privacy Implications /Legal Considerations**. Are there clear implications with regard to privacy associated with the countermeasure? Any hidden implications? What other possible legal implications exist—regulatory, reporting, conflicts of jurisdiction, etc.?

A cadre of experts throughout the sector will be assembled to evaluate each countermeasure's constraints and considerations. For instance, while financial analysts will be well positioned to ascertain the option's cost to the sector, the same analysts may not have the vantage point to render an opinion on the sector's capability to execute the option. In addition, a wide array of physical, process, and institutional experts will also be required to assess their level of confidence in each of the countermeasure's predicted effectiveness.

3.7 SBRM Step 3B: Asset Screen



For each system that is screened in, individual component assets will be identified for examination. The benefits of this approach are a clear connection between the risk objective, the supporting system, and the asset. This approach recognizes the context-specific nature of criticality and helps to reach a point where asset criticality can be demonstrated.

The SBRM asset screen serves as a filter to identify and characterize the most critical assets relative to the SRO. To that end, this step relies on a high level of consequence, or the worst reasonable damage that an asset could suffer as a result of being attacked by a terrorist or being exposed to a natural disaster, to make decisions about which elements of the network are studied in further detail.

This ability to provide context adds a new dimension to the options the sector has in prioritizing actions in response to the materiality of a risk.

3.7.1 Identify Assets

Step 3A will identify the system of interest, but that system is made up of nodes and links that are effectively the assets needed to be examined. The input from step 3A needs to be translated from the context of systems (which step 3A focuses on) to the context of assets. So, the first substep in 3B is to determine the elements that comprise the system under study from step 3A of the SBRM process by taking the system configuration and documenting the nodes and links as assets.

3.7.2 Filter Assets for Criticality

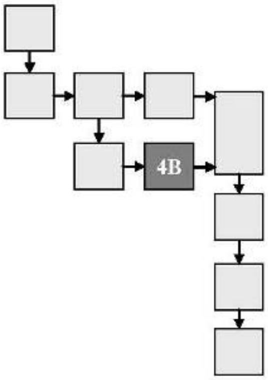
The second substep in 3B is to determine the worst reasonable damage that an asset could suffer or cause as a result of being attacked by a terrorist or being exposed to a natural disaster. By understanding the damage, or consequences, that could be inflicted on any given asset, the sector will ultimately have a more thorough understanding of where to focus its risk analysis activities and associated countermeasures. Historical evidence and other qualitative analysis methods can be used to develop the consequence scenarios.

To fully understand the worst reasonable damage that can be caused to an asset, a number of consequences may need to be evaluated to determine their relative impact. Four key indicators provide a qualitative measure of the impact of each consequence. These consequence criteria are assessed subjectively and include:

- Health impacts;
- Economic impacts;
- Mission impacts; and
- Public confidence impacts.

A rating index will be used in this step to determine which assets will be studied further. Those assets with associated consequences that meet or exceed a predetermined threshold will be selected.

3.8 SBRM Step 4B: Asset Assessment



The SBRM Asset Assessment deploys an analytical approach that seeks to develop countermeasures to reduce the risks to those assets that are critical to the sector's SROs. To that end, step 4B involves three main substeps, which are described in detail later:

1. Consolidate assets;
2. Evaluate threats, vulnerabilities, and consequences (TVC) against each asset; and
3. Develop countermeasures at the asset level.

The SBRM Asset Assessment is similar to other risk assessments in that it estimates the chances of a specific set of events occurring and/or their potential consequences.[13] Risk assessments carry a range of interpretations that vary within industries. Also, the fundamental understanding of what properly constitutes the risk assessment process can vary.[14] In the context of homeland security, risk assessments typically focus on threats, vulnerabilities, and consequences (TVC), as shown in figure 3-7.

Figure 3-7: Relative Risk as a Function of Threat, Vulnerability, and Consequence

$$\text{Relative Risk} = f\,(\underbrace{\text{Threat, Vulnerability,}}_{\textit{Likelihood of a Successful Attack}}\ \underbrace{\text{Consequence}}_{\textit{Cost/Impact of a Successful Attack}})$$

Separate analyses are associated with each term (e.g., threat analysis and vulnerability analysis). A set of activities represent the TVC analyses and are inputted into a resulting risk assessment model. The output of a risk assessment model provides a relative scoring, either qualitative or quantitative, for the assets under study. Today, several agencies have developed risk assessment models that evaluate

[13] "Risk Analysis," *Social Science Encyclopedia*, Kunreuther, 2004.

[14] A.J. Ignatowski, Ph.D.; I. Rosenthal, Ph.D.; L.D. Helsing, Ph.D., *An Internet Thesaurus/Dictionary for Analyzing Risk Assessment Processes, Laws, and Regulations*, 1997.

the TVC functions of the risk equation. Among some of these models are Analytical Risk Management (ARM), Maritime Security Risk Assessment Model (MSRAM), and Risk Analysis Methodology for Critical Asset Protection (RAMCAP).

Step 4B evaluates risk to the critical assets from steps 3B and 4A through a systematic TVC analysis. This risk assessment enables the development of outcome-focused countermeasures designed to reduce the overall risk to the assets under study. Furthermore, since step 4B is an asset-focused component of the larger SBRM, some of the assets requiring countermeasures as a result of the system assessment in step 4A are modeled to determine their effectiveness relative to the performance of the system under study.

3.8.1 Consolidate Assets

Step 4B examines, in detail, the assets that support the SRO. Assets that fit this category come from two primary sources in the SBRM—steps 3B and 4A. In addition, recognizing that these sources may not be collectively exhaustive in terms of critical assets, additional assets must be accounted for and included based on expert judgment. The first element in this activity is to pull the sets of assets from these sources and create a master list of assets that will be examined.

3.8.2 Evaluate Threats, Vulnerabilities, and Consequences Against Each Asset

Step 4B focuses on systematically analyzing specific TVC for each asset. Identifying threats and their likelihood enable a thorough understanding of the potential threats that may negatively impact assets. Vulnerability analyses build on this understanding by providing an assessment of security weaknesses that would allow certain method target pairings to succeed, providing the necessary information to determine the likelihood of success for *specific* threats. Finally, an asset's consequence analysis describes the potential results, or impacts, of a threat successfully penetrating any given asset.

After defining threats and analyzing asset vulnerabilities and the possible consequences to an asset, a risk model is used to calculate the overall risk to the asset. The risk calculation is a function of the TVC scores. This aggregated value provides a relative score that can be used to compare each asset.

For the purpose of this analysis, risk is calculated for each asset and compared relative to the score of the other assets.

3.8.3 Develop Countermeasures at the Asset Level

The previous substep provides the processes necessary to develop a comprehensive risk score for each asset. Following this calculation, additional analyses are required to determine those assets that are out-of-bounds with regard to the acceptable risk range. These assets need to be identified, reviewed, and provided countermeasures that can reduce their risk score to a more acceptable range. The candidate countermeasures associated with step 4A, System Assessment, while beneficial for the asset, are input back to step 4A for additional consequence modeling.

3.9 Supporting Activities for Steps 3 and 4

Asset-level assessments are performed at multiple levels and by various stakeholders.

3.9.1 Government Asset-Level Assessments

Federal assessors across the various modes and agencies conduct a comprehensive program of scheduled on-site facility security assessments and inspections to evaluate facilities based on risk and regulation. Their focus is on assessing risk to "highly critical" assets and systems, specifically those areas that fall outside the responsibility of the private sector.

The sector uses these assessments to review and verify infrastructure data, which may be shared among Federal partners. Using a wide variety of general and mode-specific assessment tools, assessors evaluate TVC and existing security measures. The assessment team provides a formalized report that will be reviewed with executive-level site managers. TSA captures results from assessments as lessons learned or best practices to assist the efforts of other stakeholders with similar vulnerabilities. The lead Federal security partner in charge of the assessment shares the results with TSA for further analysis.

3.9.2 Facilitated Asset-Level Assessments

These assessments enable State, local, tribal, or private sector stakeholders to use government assessment tools, training, and technical expertise to assess their infrastructure. The goal is to build capacity beyond the Federal Government for owner/operators to effectively assess their risks and aid the sector in acting on that information. Facilitated assessments offer increased access to accurate assessment data, improved comparability by using standard government tools, and opportunities to build relationships with owner/operators. TSA will capture the results from assessments as lessons learned or best practices to assist the efforts of other stakeholders with similar vulnerabilities. Finally, the lead Federal security partner in charge of the assessment will share the results with TSA for further analysis.

3.9.3 Owner/Operator Asset-Level Self-Assessments

State, local, tribal, and private sector stakeholders will also conduct assessments of their infrastructure according to their own needs or as required by law. These assessments will focus primarily on the vulnerabilities unique to the infrastructure for which they have responsibility. As a component of the top-down/bottom-up approach discussed in section 1, these assessments aid in criticality screening.

In addition to securing their facilities in the name of insurance or business continuity, stakeholders may also demonstrate national pride and civic obligation to protect their workforce, communities, and customers by completing assessments. The Federal Government will support State, local, tribal, and private sector leaders by engaging in an effort to communicate, publicize, and encourage the use of risk assessments regardless of whether the data are ever shared beyond the fence line of the owner/operator.

Assessments within this owner/operator community are not tied to using any one tool or methodology, but instead may rely on the tools and methodologies best suited to their unique needs. For those new to the sector, or new to conducting risk assessments, the SCC may provide a list of recommended best practices, tools, and methodologies. Additionally, the Federal Government will provide access to appropriate Web-based tools for assessments, as well as educational materials on the definitions of consequence, threat, and vulnerability.

3.9.4 Assessments for Cyber Networks

The cyber networks supporting the transportation system are very similar to the other systems under consideration. However, the accessible and networked nature of the cyber infrastructure results in an environment prone to internal threats, external attacks, and human error. Cyber threats are constantly evolving, with attacks by non-traceable actors that do not necessarily conform to historical event patterns. Based on these factors, it is in the best interests of sector stakeholders to focus on cyber risk assessment as a distinct effort.

NIST, the Information Systems Audit and Control Association (ISACA), the International Organization for Standardization (ISO), and a number of other organizations have documented and distributed detailed technical checklists, risk assessment checklists of controls, and information security management systems best practices. Based on regulatory requirements, sector members from the Federal, State, and local levels are often required to use the NIST *Self-Assessment Guide for Information Technology Systems*, Special Publication (SP) 800-26 and the NIST *Recommended Security Controls for Federal Information Systems*, SP 800-53 to assess levels of vulnerability and risk.

The private sector will be encouraged to use the Control Objectives for Information and Related Technology (COBIT) methodology, which is sponsored by ISACA. The COBIT methodology is aimed at assessing management standards, and may be used in conjunction with the NIST assessments commonly used by the Federal Government or NIST eScan,[15] which was developed for the private sector. Sector partners are encouraged to report security incidents to the United States Computer Emergency Readiness Team (US-CERT).

International partners will be encouraged to use the assessment methodologies referenced above, or ISO 27001 and ISO 17799, which are intended to be used together.

3.9.5 The Top 100 List

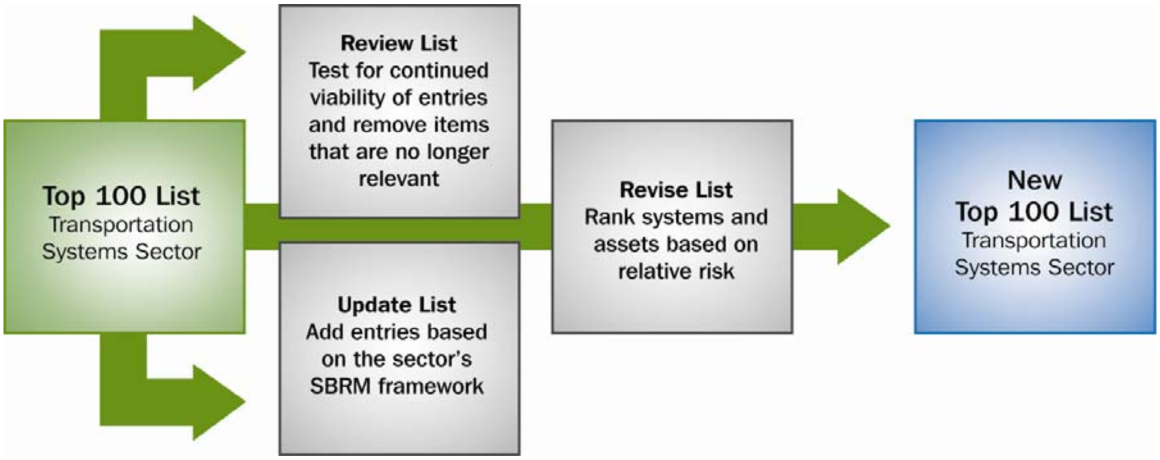
In fiscal year (FY) 2005, the DHS IP requested sectors, including the Transportation Systems Sector, to develop Top 100 asset lists, which served as a Buffer Zone Protection Program (BZPP) decisionmaking tool. With the addition of systems and networks in the NIPP, it is expected that the future content of this list will expand to include many system entries.

SBRM includes an element that focuses on annually updating the sector's Top 100 list. The update will be based on the insights developed through the implementation of the SBRM process. Specifically, the process for updating the list will use the previous year's list as a starting point. The list will be reviewed to include updated information from the SBRM process to help guide the sector's decisionmaking process. Entries that are no longer at a high enough relative risk level to warrant the continued attention that the Top 100 list provided will be removed.

The major steps involved in updating the list are presented in figure 3-8.

[15] The NIST eScan Security Assessment is a diagnostic tool designed to assess the electronic security infrastructure of a small business and provide an action plan for improving it. This tool will provide a set of recommendations to correct security problems, and will help develop a more secure model for future eBusiness strategies and positioning.

Figure 3-8: Substeps to Update the Top 100 List


Top 100 List
Transportation Systems Sector
Review List
Test for continued viability of entries and remove items that are no longer relevant
Update List
Add entries based on the sector's SBRM framework
Revise List
Rank systems and assets based on relative risk
New Top 100 List
Transportation Systems Sector

As shown in the figure, the first substep is a completed scrub of the existing list to check for entries that can be removed. This could be for any number of reasons, but the decision to remove an entry must be done with a clear indication of the rationale for the decision. The scrubbed list is then used as the basis for additions derived from the SRO-driven analysis.

SBRM steps 3B and 4B will result in the identification of assets within the national transportation system that are critical to a given SRO. In many cases, these assets will already be included in the Top 100 list, but in the event that a different asset is identified through the process, it will be considered a candidate to be included in a revised Top 100 list.

In addition to the assets, the SBRM process will identify critical systems and networks. SBRM steps 3A and 4A will result in the identification of the networks and systems associated with the SRO. All of these systems and networks will be considered as candidates to be included.

After the candidate asset, systems, and networks are identified, they will be ranked by relative risk. To do this, a heuristic rule set will be applied to decide whether to include the asset on the list, or to include the larger system within which the asset resides. The entire system belongs on the list if:

- Countermeasures are more aptly applied across the entire system to mitigate the risk as opposed to just at the critical asset(s).
- There are many assets related to greatest risk(s) versus a small number of critical assets within the system. For example, if the risk is associated with an improvised explosive device (IED) killing passengers on a train, there are a large number of places within the train where that can take place. Assuming there aren't a few places where the deaths are much higher (like in an underwater tunnel), it makes more sense to place the entire system on the list rather than each passenger station/train car.
- The risk scenario being considered involves attacking the entire system (e.g., the Mississippi River bridge system) as opposed to a single asset (e.g., a single bridge along the river).

Alternatively, a single asset belongs on the list if:

- It is the critical node within the system.
- Countermeasures would generally be applied at the asset, not the system.

4. Prioritize Risk Management Options

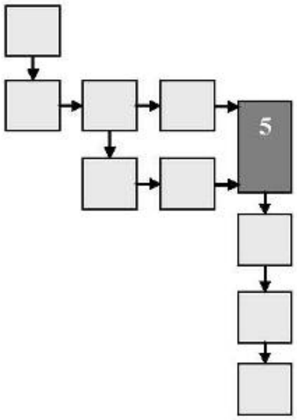
4.1 Introduction to Prioritization

While the Federal Government continues to make significant investments to improve transportation security, it is not possible to eliminate all the vulnerabilities from all transportation systems throughout the country. The uncertainty of system behavior means that perfect security is not possible. Therefore, it is essential to make strategic improvements based on prioritized risk management options according to system risk.

The first step in prioritizing risk is acknowledging that the sector's approach to risk must be system-based. Such an approach calls for a systematic decision process by which the cost, time, and other characteristics of potential solutions (along with the potential impact to the network) of the various mitigation and countermeasure options available are compared and contrasted. This analysis enables decisionmakers charged with protecting the transportation network's security to prudently develop strategies, investments, actions, and resources to effectively manage risk. After developing solutions, strategy must be effectively translated to action. Stakeholders must evaluate the sector's portfolio of programs effectively by rigorously tracking cost, schedule, and performance to ensure success.

The sector-wide analyses and prioritization are in no way intended to remove the budgetary discretion of individual agencies in managing their budget. Among agencies across the sector, determinations and prioritizations on which security programs merit additional funding shall be advisory in nature, and considered along with other priorities within each agency's budget development process.

4.2 SBRM Step 5: Countermeasure Prioritization



The countermeasures that emerge from steps 4A and 4B have been scored and ranked according to their effectiveness against the SRO. However, these rankings alone do not result in effective, cost-efficient solutions. The interactions and net effects of countermeasures must be considered before strategies can be translated to effective action plans. For example, if one highly ranked countermeasure from step 4A overlaps with, or even negates, another highly ranked countermeasure from step 4B, its collective effectiveness will decrease. Alternatively, a package that incorporates countermeasures that are complementary to each other could result in an increased collective effectiveness at a reduced cost.

As a result, in step 5, working groups are formed to identify ways that effective countermeasures can be packaged together to achieve the SRO. Once these countermeasures are identified, the working group will score and rank each package's cost and overall effectiveness. These comparative rankings will allow the sector to identify the countermeasure packages that experts have judged to be most effective in helping decisionmakers build balanced, focused, high-impact countermeasure programs in step 6. The three main substeps associated with step 5 are:

1. Develop decision framework;
2. Package countermeasures; and
3. Rank countermeasure packages.

4.2.1 Develop Decision Framework

The first substep in step 5 is to select experts to develop the decision frameworks necessary to identify and prioritize countermeasure packages. It is essential that these working groups are composed of a knowledgeable and diverse cadre of subject matter experts to evaluate the array of potential countermeasure packages. Next, a method to rank the packages, taking into consideration the relative importance of each in achieving the SRO, will need to be established.

4.2.2 Package Countermeasures

Before the new countermeasure packages are identified, the sector must identify existing efforts that may contribute to SRO achievement. These existing efforts may be incorporated into countermeasure packages to ensure that the packages balance existing activities with the introduction of new ones. This means existing efforts may require replacement or elimination if their performance no longer supports the agency's priorities.

The working groups will assemble well-informed packages by analyzing countermeasure synergies, redundancies, timing issues, and other considerations. It is important that countermeasure packages are developed to address the entire portfolio associated with the SRO. Furthermore, at this point in the process, it is also necessary to consider a variety of different packaging strategies, as an evaluation of constraints and other considerations may drive the need for an analysis of a wide array of potential solutions.

4.2.3 Rank Countermeasure Packages

After establishing the decision framework and developing the packages, experts must evaluate the relative impact of each countermeasure package against the SRO and estimated cost to implement.

It is essential that the established working group possess the domain and functional expertise necessary to make well-informed judgments. For example, countermeasure packages seeking to mitigate risk through institutional (e.g., regulations) and process changes may require a different set of experts than those aimed at improving the physical integrity of assets.

The first step in the scoring process is to determine the relative effectiveness of each countermeasure package. Surveys, voting, discussion, and consensus among experts may be helpful to make well-informed decisions.

Next, the estimated cost to implement must be evaluated. While it is necessary to assign cost scores to countermeasure packages, detailed cost analyses are not required at this point in the SBRM process. Finally, once the effectiveness and cost scoring exercises have been completed, the countermeasure package scores are adjusted according to the SRO.

Once these scores are calculated for the countermeasure packages, a review committee will verify the scores that were given to the countermeasure packages. The verification process ensures that any "groupthink" that might emerge from working group sessions is corrected.

When the scores are verified, a ranked, prioritized list of countermeasure packages will be compiled. While these effectiveness rankings are useful for identifying cost-effective countermeasure packages, they alone cannot determine which countermeasure packages should be incorporated into programs. Key considerations and constraints must be evaluated.

4.3 Support Activity for Step 5

Although the cyber risk management prioritization process fits within the SBRM framework, the unique challenges of cyber risk require specific mention.

4.3.1 Cyber Prioritization

Sector members will be responsible for performing prioritization of critical cyber assets and reporting relevant metrics as requested by sector working groups. Stakeholders should utilize NIST Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, which provides guidance for prioritization and addresses a tiered approach to segment the items into high, medium, and low categories.

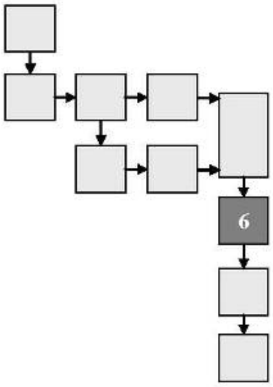
5. Develop and Implement Security Programs

5.1 Overview of Sector Security Programs

In the wake of September 11, 2001, security measures implemented across the sector were selected using a variety of approaches. For example, the freight rail industry conducted a vulnerability and risk analysis using Federal Government, industry, and international best practices. The result of this effort was the Railroad Terrorism Risk Analysis and Security Management Plan. Simultaneously, individual owner/operators began implementing a variety of security programs or individual security measures, sometimes based on widely accepted risk assessment methodologies.

Building on earlier efforts, all sector security partners will continue working together to develop an overarching portfolio of risk-based security programs and countermeasures to improve the sector's risk profile. TSA will facilitate the development and implementation of security programs by coordinating with stakeholders through the GCC and SCC to manage risk by minimizing consequences, mitigating vulnerabilities, and deterring threats. Each partner is responsible for developing protective programs that are risk-based, coordinated, scalable, and cost-effective to their individual organizations. TSA will work with the DHS NCSD to ensure that the sector partners are informed about available cyber protection program methodologies.

5.2 SBRM Step 6: Countermeasure Program Development



In step 6, the prioritized countermeasure packages that emerged from step 5 will be scored according to their overall value and organized into balanced, focused countermeasure programs. The overall value of such programs is determined by comparing the effectiveness scores from step 5 to the constraints and considerations that may impact each program's effectiveness, such as organizational capability, internal cost, and time to implement. Once completed, the sector will conduct a top-down review of the programs to ensure that other factors, such as stakeholder concerns, are considered and incorporated into the final set.

In short, the countermeasure program refinement and vetting process allows sector management and decisionmakers to ensure that the programs are focused, realistic, and aligned with strategic management considerations.

5.2.1 Assess Constraints and Considerations

A well-informed selection of countermeasure programs requires a complete understanding of the costs, constraints, and considerations associated with their implementation.

One of the most important constraints impacting countermeasure packages is available funding. As a result, step 6 begins with identifying SRO budget ranges. These ranges will be an important factor in the portfolio optimization process.

The second substep is assessing other key constraints and considerations affecting countermeasure program value. In step 4A, a high-level analysis of constraints was conducted for each countermeasure. As previously stated, constraints and considerations could include:

- Internal government cost;
- Cost to industry;
- Level of confidence in countermeasure;
- Likelihood of success/difficulty;
- Sector capability;
- Time to implement; and
- Privacy implications/legal considerations.

To assess these constraints and make judgments on their impact on program effectiveness, working groups will create a framework to guide the constraints analysis. This framework will state what types of constraints and considerations should be assessed. For example, a particularly sensitive SRO to prevent terrorist attacks on critical systems could include countermeasure packages that might raise privacy concerns from citizens or sector stakeholders. As a result, this constraints analysis framework may include privacy as a key consideration to be assessed.

Once key constraints categories are determined, the working group will assign relative weights to each. These weights should reflect the requirements of each SRO. For example, a particularly time-sensitive SRO might place a high weight on the length of time required to implement.

With the constraints analysis framework finalized, the working group will assess the factors impacting each countermeasure package's effectiveness. To conduct the analysis, the working group will consider expert opinion, historical data, and feedback from strategic sources.

Once these constraints and alternatives are documented, the working group will determine the degree to which the constraints impact countermeasure package effectiveness. Similar to the scoring in step 5, a number of methods—surveys, voting, discussion, and consensus—can be used to conduct the scoring exercises.

The scores that result from this exercise will be aggregated and weighted for each countermeasure package. The sum of the constraints scores can then be evaluated against the effectiveness rankings developed in step 5. The sum of the two can be described as the countermeasure package value.

5.2.2 Build Countermeasure Programs

Countermeasure programs should consist of groupings of countermeasure packages that are thematically linked and their collective impact is sufficient to substantially meet SRO goals. The first activity in building countermeasure programs will be to align the countermeasure packages with the highest value to the SRO that they were designed to achieve. Next, the overall impact of constraints and considerations will need to be evaluated to determine each package's feasibility. Those packages perceived to be the most effective in accomplishing the SRO may need to be augmented to address the constraints evaluated earlier in the process.

5.2.3 Review Countermeasure Programs

Once the SRO countermeasure programs are developed, sector leadership will conduct a top-down review of the recommendations, taking into consideration management perspectives. It is important to note that the analyses supporting the proposed programs provide an overarching framework for decisionmakers, but does not substitute experience and institutional knowledge. For example, it may be determined that even though the sector does not currently have the organizational capability to implement a very costly, but potentially effective countermeasure package, the positive effects of that countermeasure package outweigh those constraints and it should be included in a countermeasure program. Alternatively, it may be determined that a countermeasure program would have such a significant negative impact on sector stakeholders that it should not be implemented, or that additional activities will be necessary to mitigate the negative impact.

The high-level review finalizes the portfolio optimization step and sets the stage for planning and deployment activities in step 7.

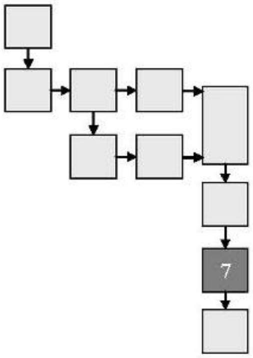
5.3 Supporting Activities for Step 6

Once assessment and prioritization of risks have been completed, a gap analysis will be performed between identified needs, existing security programs, and progress toward achieving sector security goals.

Discussion of the Risk and Strategy Matrix (RASM) provides the necessary structure to ensure that the Transportation Systems Sector is effectively making progress toward measurable outcomes. RASM assists in gap analysis by helping to inform the sector as to whether the SRO has adequate security measures across the set of sector goals.

GCC and SCC partners will collaborate to identify the capabilities the sector currently has that could be used to mitigate the identified risk. If the capability does not currently exist, TSA will lead an examination of other programs (including grants) that may be adapted to address the need or direct R&D activities to design new capabilities. Because of the likelihood that potential risk gaps may involve areas where numerous interdependencies are present, TSA will work with other sector lead agencies to identify and leverage potential programs as warranted.

5.4 SBRM Step 7: Deployment Engine



In step 7, the SRO countermeasure portfolios that emerged from step 6 are transitioned into sector planning and budgeting activities. To achieve this alignment, countermeasure program plans are developed that outline the roles and responsibilities necessary to resource, manage, and oversee their implementation.

These alignments provide stakeholders with a clear link between their respective program portfolios and the sector's SROs. This link will be further detailed in step 8, as measures are developed that assess the degree to which countermeasure programs are contributing to SRO achievement. The following substeps align with the Federal Government's Planning, Programming, Budgeting, and Execution (PPBE) activities. It is important to note that the process described below is not intended to replace the existing budget processes of sector stakeholders, but rather relate SBRM methodology, specifically SROs, to their current budgetary planning activities.

5.4.1 Develop Program Plans

The countermeasure programs that emerge from step 6 indicate the investments that the sector has determined will be most effective in supporting achievement of the SROs. Simply stated, while these programs indicate *what* needs to be done, they do not describe *how* to do it. As a result, the initial substeps in step 7 focus on creating plans that describe the activities necessary to initiate and implement the countermeasure programs and coordinate responsibilities within the sector.

Program plans will outline which stakeholders are likely to have management responsibility and authority to oversee countermeasure program implementation and to what degree the programs will require coordination with Transportation Systems Sector security partners. They will also provide the budget estimates for activities under the countermeasure program and their respective implementation milestones. In addition, the program plans will also detail specific activities necessary to mitigate the implementation constraints identified in step 6 of the SBRM process.

5.4.2 Coordinate Program Plans

At this point, the program plans are initial projections of who will be responsible for managing and overseeing countermeasure program implementation. Coordination between sector partners is key to ensuring that program plans avoid duplicative or conflicting countermeasures, defining clear roles and responsibilities, and driving collaborative efforts.

5.4.3 Integrate Program Plans Into Budgeting Processes

Each security partner (Federal, State, and local governments, and the private sector) has its own unique budgeting process for determining, rationalizing, and approving funding levels for security programs and initiatives. In this substep, the Federal budgeting processes will determine appropriate funding levels for its programs and initiatives. Once Federal funding levels are determined, decisions can be made on how to allocate available Federal resources and used to inform the State, local, and private sector budgeting process. If budget gaps are identified, decisions should consider the criticality of the countermeasure programs to accomplishing the SROs and the impact that a gap in countermeasure program funding would have on SRO achievement.

As a result of step 7, sector strategies and budgets will be aligned and integrated with the sector's highest priorities. This integration allows sector stakeholders to clearly understand, at a high-level, how their organization and operation unit portfolios impact and link to countermeasure programs and SRO aims. This understanding of program/SRO alignment is critical to step 8, in which performance measures are developed that detail how countermeasure program implementation contributes to SRO achievement.

The sector-wide analyses and prioritization are in no way intended to remove the budgetary discretion of individual agencies in managing their budget. Among agencies across the sector, determinations and prioritizations on which security programs merit additional funding shall be advisory in nature, and considered along with other priorities within each agency's budget development process.

5.5 Support Activities for Step 7

A number of existing programs and activities will act as key sources of information for the overall SBRM process. The supporting activities listed below remain essential tools in the deployment process.

5.5.1 Cyber Programs

Sector partners are responsible for implementing their own cyber security programs. TSA will coordinate through the GCC and SCC communities and with NCSD to provide online, annual, in-person forums for sector members to share their best practices in IT security and other security programs. The SCC will play a key role in communicating and implementing new programs to ensure the resilience of transportation cyber networks.

TSA coordinates efforts with US-CERT through notifications of incidents affecting TSA and by reviewing bulletins distributed by US-CERT. Other Federal partners and the private sector are encouraged to take advantage of the information shared by US-CERT.

TSA meets with NCSD and the Chief Information Security Officers (CISOs) from various government agencies to develop best practices. TSA will continue to work with NCSD to ensure that TSA and the sector's cyber protective programs are aligned with NCSD's goals for the IT sector and follow best practices developed by NIST and the ISO.

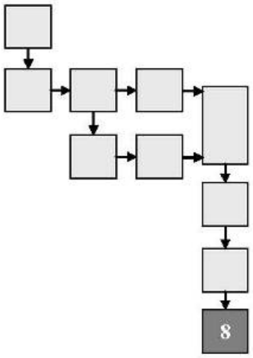
The cyber protective programs recommended in this section are intended to be used as self-assessments. Many of the programs result in an executive report or summary data that is analyzed by cyber security professionals. To measure protective programs, stakeholders will be asked to share their baselines, their performance goals, and their ability to achieve performance goals. For stakeholders who may need more guidance in this area, TSA will coordinate with NCSD to develop a list of recommendations and points of contact that can provide additional guidance.

5.5.2 Security Program Maintenance

Maintenance of security programs—and their continued contribution to the sector's resilience strategy—is a shared responsibility. Duties associated with this responsibility will vary with the security program and the scope of the program's goals. Maintaining federally operated and managed programs is the responsibility of the designated lead Federal partner. If the security program is developed and managed at a regional or local level, owners and operators at that level are responsible for maintenance. TSA will coordinate and communicate with stakeholders to ensure that any changes impacting other programs or planning efforts *at any level* are properly explained and efficiently carried out (this may include, for example, grants to State departments of transportation or State Homeland Security Advisors).

The success of any security program is based, in large part, on the input and cooperation of relevant stakeholders. The GCC and SCC will play essential roles in monitoring the success of each program to assess and justify continued maintenance of programs over their life cycle. The councils will work with the Measurement Joint Working Group to ensure that performance measures are reviewed and updated as necessary. The lead Federal partners for each security program will be responsible for providing standardized feedback and conducting an annual survey on the effectiveness and efficiency of their programs. This feedback will be used to guide program continuation or adjustment, as well as to collect best practices and lessons learned in developing new programs.

5.6 SBRM Step 8: Performance Measurement



In the eighth and final step of the SBRM, the sector will identify and implement meaningful performance measures that track the progress and effectiveness of countermeasure programs in achieving the sector's SROs. These performance measures empower stakeholders to track whether their program portfolios are behind or ahead of schedule and observe the degree to which their activities are supporting the achievement of the SRO.

Monitored, collected performance measures also enable executives to communicate progress toward SROs to Transportation Systems Sector security partners and oversight entities. In addition, the findings that result from these measures will lead to continuous improvements in future iterations of the SBRM.

5.6.1 Map Desired Activities, Outputs, and Outcomes for Each Countermeasure

To conduct these evaluations, measures of effectiveness must be developed and monitored for each countermeasure program. These effectiveness measures flow from maps of activities, outputs, and outcomes—also known as performance logic models.

5.6.2 Develop Performance Measures and Data Requirements

Output and outcome performance measures will emerge from developing countermeasure program performance logic models. These measures will be used to monitor the degree to which countermeasure programs are achieving their objectives. Output measures will assist in analyzing the program's ability to meet the milestones, while outcome measures will gauge a program's contribution to the sector's SROs.

As these performance measures are identified and documented, the types of data that need to be collected to perform the evaluations will also be identified.

5.6.3 Develop Data Collection, Verification, and Reporting Processes

Based on the data requirements identified in the previous activity, the sector will develop a data collection plan for each countermeasure program. The data collection plan should define what data needs to be collected to inform each performance measure, how frequently this data should be collected and, perhaps most importantly, what resources will be required (e.g., analytical tools and methods) to collect the data.

5.6.4 Link Sector Measures

Once the performance measures are identified and data collection plans completed, performance management responsibilities will be agreed to by sector stakeholders. This is particularly important because during the life cycle of a given countermeasure program, output and outcome measures may reveal best practices, improvement areas, and opportunities for management intervention.

The overall measurement of the performance for the Transportation Systems Sector is discussed in detail in section 6, Measure Progress.

6. Measure Progress

6.1 CI/KR Performance Measurement

An effective NIPP performance measurement program begins with the collaborative development of metrics to measure progress and performance. A formal Measurement Joint Working Group, created under both the Transportation Systems GCC and SCC and under the leadership of TSA's lead measurement organization, will operationalize measures, establish data sources, establish data collection and verification procedures, set measurement policy for the Transportation Systems SSP, and approve supporting procedures. The Measurement Joint Working Group will be composed of transportation subject matter experts from each mode, sector risk leaders, sector cyber security leaders, GCC and SCC measurement leaders, private sector data store leaders, and invited measurement professionals.

The Measurement Joint Working Group will communicate regularly with both the GCC and SCC members and will ensure that working group progress and plans are fully transparent and have the cooperation of GCC and SCC members. In addition, work products of the Measurement Joint Working Group will be submitted for approval, when appropriate, to the overarching Transportation Systems GCC and SCC, the DHS, and NCSD. Expected benefits of the group include minimizing the risk in measure selection, promoting measurement efficiency by leveraging existing private and government data stores, promoting cross use of NIPP measures to meet OMB measurement requirements, providing decision-quality information for NIPP Annual Report analysis, and ensuring effective measurement approaches that produce results with the least impact on stakeholders.

6.2 Developing Metrics

6.2.1 Use of Core Metrics Defined by the DHS

The core metrics, common across all sectors, are a set of descriptive and output metrics that measure progress made by all CI/KR sectors in implementing the NIPP risk management framework. The DHS develops the core metrics and communicates them to the SSAs. A sample of the current core metrics reported includes:

- Total number of assets by class (mode);
- Percentage of medium- and high-consequence assets rated as high risk;
- Percentage of formal security partner agreements by sector and geographic location; and
- Percentage of assets reduced from high risk.

The complete list of core metrics is likely to evolve over time and be much larger. The DHS will also identify cyber security core metrics.

6.2.2 Development of Sector-Specific Measures

In addition to core metrics, the Measurement Joint Working Group will develop sector-specific metrics to more thoroughly evaluate sector progress and drive continuous improvement in achieving the goals and objectives determined by the sector.

There are two types of sector-specific metrics:

- Metrics associated with Transportation Systems Sector goals and objectives; and
- Metrics associated with Transportation Systems Sector programs.

Sector-specific metrics also will include both common and tailored cyber security measures. In addition, metrics associated with the SROs within the sector's SBRM methodology will focus on driving continuous improvement of the SBRM process.

6.2.3 Metrics Associated With Sector Goals (Outcome Measures Associated With Sector Goals and Objectives)

The sector-specific measures associated with sector goals and objectives are proposed to be outcome measures. Proxy (interim output) measures may be required as stand-ins for outcome measures in the early years of the program when baseline data are being acquired. The outcome measures will monitor *information on effects*[16] related to meeting sector goals and objectives. The Measurement Joint Working Group will execute the published Outcome Monitoring Technique[17] for each sector goal and objective combination as follows:

Step 1: Working top-down, document the outcome measurement logic model.

Step 2: Translate near- and intermediate-term outcomes into outcome measures.

Step 3: Operationalize the outcome measures using existing data when possible.

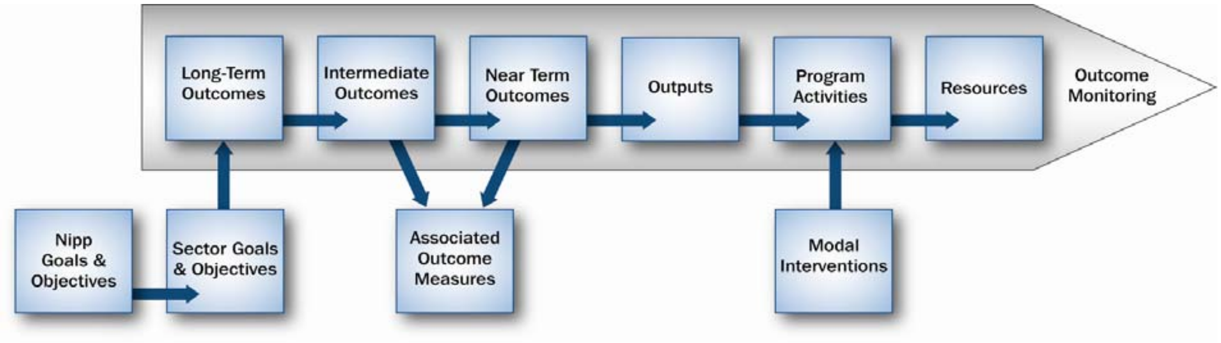
Step 4: Commence ongoing (year after year) measurement.

The steps are captured in figure 6-1.

[16] In the evaluation literature, measures of effectiveness or *effect* mean how much change can be attributed with some degree of confidence to the concept being measured. Empirical techniques, such as the Randomized Controlled Trial advocated by OMB, are the only program measurement techniques that allow one to determine *with high confidence* the size of an *effect* attributed to an intervention (i.e., program).

[17] For further information on the Outcome Monitoring Technique, see "Measuring and Monitoring Program Outcomes," in Rossi, Peter H.; Lipsey, Mark W., et al., *Evaluation: A Systematic Approach*, 7th edition, Thousand Oaks, CA: Sage Publications, 2004, pp. 203-233. Per Rossi, et al., pp. 224-225, "… [O]utcome monitoring provides useful and relatively inexpensive information about program effects, usually in a reasonable time frame. … Because of its limitations, however, outcome monitoring is mainly a technique for generating feedback to help program managers better administer and improve their programs, not one for assessing the program's effects" on the conditions the program is intended to improve. The Outcome Monitoring Technique, while not empirical, also may be useful for identifying *effect* in areas, such as security, where there are believed to be few competing alternative explanations or interventions.

Figure 6-1: Outcome Measurement Logic Model



In addition, for the sector goal *enhance information and intelligence sharing among transportation sector security partners*, the Measurement Joint Working Group will document, for GCC and SCC coordination, how the implementation of this goal and associated objectives will satisfy the requirements of Executive Order 13416, Strengthening Surface Transportation Security. This Executive Order is expected to request annual reviews of the effectiveness of surface transportation system-related, information-sharing mechanisms.

6.2.4 Metrics Associated With Transportation Systems Sector Programs

Each year, both the Transportation Systems GCC and SCC will identify the most significant and innovative programs within the sector believed to have the greatest potential for improving security within the sector. For these model programs, which will be documented in the annual report, the Measurement Joint Working Group will coordinate with program owners to develop and operationalize a program-specific set of measures and reporting schedule. At a minimum, each model program will have one outcome measure, one cost-effectiveness measure,[18] one risk-reduction impact measure, and one efficiency (if required by IP) measure. Additional measures derived using conventional performance measurement (performance indicator monitoring) techniques also are possible.

Included GCC security programs already may be measured as required by the Government Performance Results Act (GPRA), the Program Assessment Rating Tool (PART), and OMB 300. GCC members will be encouraged to use existing measures to the maximum extent possible, but are permitted to augment existing program measurement practices with incremental practices adopted to support sector annual report requirements, if deemed appropriate by each individual agency.

6.2.5 Strategic Risk Objectives Measures

The Transportation Systems GCC and SCC are expected to request the Measurement Joint Working Group to also measure progress toward meeting selected SROs. SROs derive from the SBRM process and will be defined more fully over time.

[18] The cost-effectiveness measure is similar to a cost-benefit measure ("we lowered risk by x and it cost y dollars"). Such knowledge can be used to evaluate performance and prioritize next steps at the NIPP level. Cost-effectiveness measures aid in evaluating whether the most cost-effective process has been employed and ensuring that a project's targets are met.

6.3 Information Collection and Verification

Information collection and verification can commence once the performance measures are operationalized. Information collection begins with identifying the data owners for each performance measure, the source of the data, the frequency of data collection, metrics assessment process and frequency, and any validation that applies to the performance measure.

Performance metrics will go through a validation and verification process. This process builds on the operationalization data to:

- Validate the data sources from which the data are obtained;
- Fully describe each performance measure;
- Validate methods and frequency for data collection;
- Describe how the data are verified (i.e., how we know that the data are accurate and timely and comparable to data from other time periods);
- State whether the data are reliable and how reliability is measured;
- Establish protocols for the data owners to validate the accuracy of the data provided; and
- Provide a complete set of metadata templates for each performance measure that captures key data points that will serve as the measure data dictionary.

Data collection will be an ongoing process. Following regular data collection, a coordinated higher level review may be conducted by an office not responsible for collecting the data. The SSA's lead measurement organization will serve as the roll-up point for measurement information received from the sector. Although this organization and its systems can handle both unclassified and SSI material, sister organizations (e.g., Risk Management Strategic Planning (RMSP) Division, OI) do handle classified material.

As the measure development, data collection, and verification processes mature, supplemental technology tools (data modeling and verification) might be considered to automate the data accuracy, reliability, and verification procedures. Statistical sampling tools can be applied to provide quantifiable information that supports the accuracy, reliability, and validity of the data supporting each performance measure.

6.4 Reporting Timelines

Core and sector-specific metrics will be reported to the DHS on a regular, predetermined schedule to ensure that they meet the DHS's need to monitor performance across all sectors. To the extent feasible, sector reporting timelines will be established to coincide with OMB and other legislative reporting requirements. The Transportation Systems Sector Measurement Joint Working Group will work with the GCC and SCC to identify, document, and implement the most effective and cost-efficient repeatable process, and establish a schedule to report core and sector-specific metrics (goal and program) to the DHS. SROs also will be reported within the sector to guide the sector's risk management program. Process definition will include evaluation of the most appropriate role for the emerging IP Metrics Web Portal platform in the final sector reporting processes.

HSPD-7 requires SSAs to provide the Secretary of Homeland Security with an annual report on their efforts to identify, prioritize, and coordinate the protection of CI/KR in their respective sectors. TSA worked in close collaboration with sector security partners, SCCs, GCCs, and other organizations in developing the 2006 Annual Report and will continue to do so for further reports. The Measurement Joint Working Group and the Transportation Systems Sector GCC and SCC will work to establish the reporting timeline and measurement requirements to support future Transportation Systems Sector Annual Reports.

6.5 Implementation Actions

The sector's security partners have identified a series of actions to be completed as the Transportation Systems SSP is implemented over the next few years. These actions, illustrated in table 6-1, represent the major actions that TSA and some members of the sector will undertake to achieve a robust, resilient transportation infrastructure. The actions listed in table 6-1 are "notional"—meaning they provide a sense of what will be accomplished over the next few years. The SCC and GCC will identify improved, more definitive milestones through collaborative discussions. Successful completion of these actions depends on the availability of public and private resources.

TSA and USCG, as the SSAs, will work with the Transportation Systems Sector GCC and SCC to undertake the responsibilities included in table 6-1. Unless otherwise stated, all milestones will be targeted in cooperation and coordination with all transportation security partners under CIPAC, including, but not limited to, TSA, the Transportation Systems Sector GCC and SCC, the DHS, and other security partners in government and industry.

Table 6-1: Milestones of Key Responsibilities Under HSPD-7

Milestone	Date	Lead Responsibility
Establish sector partnership coordination processes to ensure that all security partners (Federal, State, regional, local, and private sector) are involved in planning efforts from their inception.	No later than (NLT) 30 days after SSP submission	SSAs
Establish process to introduce NIPP implementation actions according to appendix 2B of the NIPP.	NLT 90 days after SSP submission	GCC/SCC
Continue to build and strengthen the role of the GCC and modal GCCs, the modal SCCs, CIPAC, and its transportation security committees and working groups to implement the Transportation Systems SSP, the modal implementation plans, and related security activities.	Underway; ongoing	GCC/SCC
Continue and expand on joint exercises with transportation security partners and other interdependent sectors.	Ongoing	GCC/SCC
Enhance information-sharing platforms, such as HSIN and ISACs, to share information on threats to the transportation infrastructure and security partners.	Ongoing	GCC/SCC

Table 6-1: Milestones of Key Responsibilities Under HSPD-7

Milestone	Date	Lead Responsibility
Develop an ongoing process for assessing compliance with any security guidelines and security requirements issued by the Secretary of Homeland Security or Secretary of Transportation for surface transportation systems and the need for revision of such guidelines and requirements to ensure their continued effectiveness.	Underway; ongoing	SSA
Convene a technical assistance seminar/workshop to review the SBRM process with sector security partners, especially Federal and private sector partners. Review existing risk/vulnerability assessment methodologies (asset/facility level, system level, and regional level) and possible future improvements.	NLT 90 days after SSP submission	SSAs
Convene joint GCC/SCC (Federal, private sector, and other entities) meeting to discuss development of SROs.	NLT 90 days after SSP submission	SSAs
Work with the DHS IP and Office of State and Local Government Coordination and Preparedness to engage State and local Homeland Security Advisors and other security representatives to determine long-range protective programs and initiatives.	NLT 90 days after SSP submission	SSA
Establish Transportation Systems SCC.	NLT 90 days after Transportation Systems SSP submission	Modal SCCs
Expand Research and Development Working Group (R&DWG) to include private sector R&D/technology community. Establish a regular schedule of joint government/industry meetings to continue overall outreach through briefings and conference participation to all transportation stakeholders and modes for reviewing existing R&D efforts and comparing results to R&D roadmaps and study recommendations.	NLT 90 days after SSP submission	SSA
Work with the Transportation Systems Sector GCC and SCC to develop sector CI/KR annual report.	July 1, 2007	SSAs
Establish SROs that identify systems-based risk priorities.	NLT 180 days after SSP submission	GCC/SCC
Update and refine the DHS Top 100 list based on the SBRM process.	NTL 180 days after SSP submission	SSAs
Organize CIPAC joint Transportation Systems Sector task force composed of GCC and SCC members to address data collection—verifying data, risk assessment methods, how data may be collected, shared and possible approaches to collect information and data during transportation emergencies using published PCII rules.	NLT 180 days after SSP submission; ongoing	GCC/SCC
Establish Measurement Joint Working Group with sector security partners under the Transportation Systems Sector GCC and SCC.	NLT 180 days after SSP submission	SSAs

Table 6-1: Milestones of Key Responsibilities Under HSPD-7

Milestone	Date	Lead Responsibility
Establish Measurement Joint Response and Recovery Group with sector security partners under the Transportation Systems Sector GCC and SCC.	NLT 180 days after SSP submission	SSA
Consider establishing Joint Intel Working Group with sector security partners under the Transportation Systems Sector GCC and SCC.	NLT 180 days after SSP submission	SSA
Establish the R&D data-gathering approach, analysis, and distribution process with joint GCC/SCC agreement to include pending surface transportation security improvements (Federal, State, local, tribal, private, and academia).	NLT 180 days after SSP submission	SSA
Establish and make available lists of available technologies and products related to the protection of surface transportation to Federal, State, local, and tribal governmental entities and to private sector owners and operators of surface transportation systems.	NLT 180 days after SSP submission	SSA
Determine product and technology needs to inform the requirements for and prioritization of RDT&E.	NLT 180 days after SSP submission	GCC/SCC
Produce classified and non-classified threat assessments by mode.	NTL 180 days after SSP submission	SSA
Develop a regional approach for a public outreach conference(s) to address R&D transportation efforts.	NLT 270 days after SSP submission	SSA
Update NADB transportation taxonomy and attributes to reflect a systems view of the transportation network.	NTL 360 days after SSP submission	SSAs
Define sector-specific performance measures.	NLT 360 days after SSP submission	SSAs

6.6 Challenges and Continuous Improvement

TSA and its fellow stakeholders are using a metrics-based system of performance evaluation to provide a basis for documenting actual performance, facilitating systematic analysis, and promoting effective management. Metrics supply the data to affirm that specific goals are being met or to show what corrective actions may be required to stay on target.

The Transportation Systems Sector GCC and SCC will develop procedures to govern sector communication. The procedures will be consistent with continuous improvement models and will include frequency guidelines.

Sector Information Communication. A structured and focused communications strategy with the sector stakeholders will foster up-to-date knowledge of the best security plans, procedures, and programs. This will contribute to greater preparedness and resilience of transportation operations. TSA, working through the GCC, SCC, ISACs, State and local Fusion Centers, and other stakeholder associations and organizations, will disseminate areas for improvement, best practices, and lessons learned. Sector partners also will work to design and implement a communications strategy that will share information through the HSIN, Lessons Learned Information Sharing (LLIS), and other Web-based networks, as well as through modal forums (e.g., SCC/GCC), subject matter expert briefings, and special events, as needed. These efforts will provide a venue for stakeholder feedback on current security SSP and program effectiveness, successes, and areas of improvement, and the efforts will suggest future areas where stakeholders would recommend development, measurement options, and R&D activities.

Transportation Systems Sector GCC and SCC Decisionmaking. Milestones will be developed to monitor the SSP and program implementation progress. In addition, performance will be reviewed and tracked year after year to measure progress toward sector goals and the status of the sector's countermeasure programs. This periodic analysis will be used to focus the sector's attention on SSA strategies that require adjustment and protective programs that warrant programmatic changes, additional resources, or redirection. As a data baseline accumulates, expert opinion may be used to establish targets and associated milestones.

Measurement Challenges. There are many technical challenges facing the measurement program and the use of measurement data. The perceived largest challenges are effectively facilitating security partner's participation, effectively managing program costs and resources, developing and improving risk-reduction measurement techniques, gathering appropriate risk baseline data, enhancing cyber expertise, ensuring quality security measurements, and effectively sharing data.

7. Research and Development: CI/KR Protection

7.1 Overview of Transportation Systems Sector R&D

The Transportation Systems Sector recognizes the importance of working in concert with the NIPP and HSPD-7. The directive calls for the Secretary of Homeland Security to establish a comprehensive, integrated National Plan for CI/KR Protection and "[i]n coordination with the Director of the Office of Science and Technology Policy, the Secretary shall prepare, on an annual basis, a Federal Research and Development Plan in support of this directive."

The National Critical Infrastructure Protection Research and Development Plan (NCIP R&D Plan)[19] was developed as a result of HSPD-7 and it established a baseline for R&D capabilities required across all sectors. Prepared by the DHS S&T and the Office of Science and Technology Policy (OSTP), the NCIP R&D Plan highlights the R&D needs as having three primary "technology-enabling" goals and nine technology-centric themes.[20]

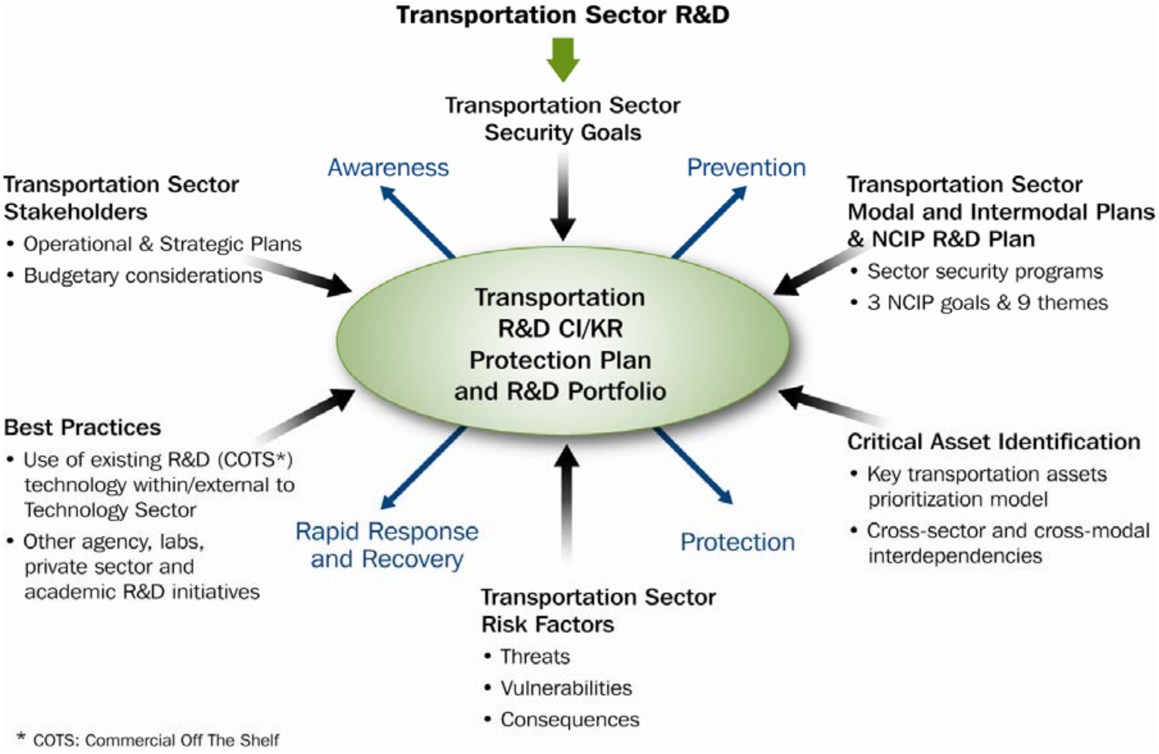
The Transportation Systems Sector's security goals support the overarching NIPP goal of a safer, more secure America and the prioritization of R&D investments. The strategic goals of the Transportation Systems SSP, together with the NCIP R&D Plan and the operational support needs of the government and private sector, provide the foundation for the sector CI/KR R&D Plan.

Figure 7-1 illustrates influencing factors in developing the R&D Plan.

[19] The NCIP Plan can be found on the DHS Web site at www.dhs.gov/xlibrary/assets/ST_2004_NCIP_RD_PlanFINALApr05.pdf.

[20] The three NCIP R&D technology enabling goals: (1) a national common operating picture for critical infrastructures; (2) a next-generation Internet architecture with security designed-in and inherent in all elements rather than added after the fact; (3) resilient, self-diagnosing, and self-healing physical and cyber infrastructure systems. The nine technology-centric themes include: (1) detection and sensor; (2) protection and prevention; (3) entry and access portals; (4) insider threats; (5) analysis and decision support; (6) response, recovery, and reconstitution; (7) new and emerging; (8) advanced architecture; and (9) human and social.

Figure 7-1: Transportation Systems SSP R&D Plan Influencing Factors


Transportation Sector R&D
Transportation Sector Security Goals
Awareness
Prevention
Transportation Sector Stakeholders
• Operational & Strategic Plans
• Budgetary considerations
Transportation Sector Modal and Intermodal Plans & NCIP R&D Plan
• Sector security programs
• 3 NCIP goals & 9 themes
Transportation R&D CI/KR Protection Plan and R&D Portfolio
Best Practices
• Use of existing R&D (COTS*) technology within/external to Technology Sector
• Other agency, labs, private sector and academic R&D initiatives
Critical Asset Identification
• Key transportation assets prioritization model
• Cross-sector and cross-modal interdependencies
Rapid Response and Recovery
Protection
Transportation Sector Risk Factors
• Threats
• Vulnerabilities
• Consequences
* COTS: Commercial Off The Shelf

7.1.1 Transportation Systems Sector R&D Landscape

R&D has always been essential to the Transportation Systems Sector and represents a primary strategy to deter and prevent terrorist actions. Ongoing challenges to sector R&D efforts include the diversity of ownership of Transportation Systems Sector assets, inherent vulnerability of surface transportation, constant evolution of transportation security, and the increasing dependency on intermodal and international transportation. For these reasons, continual involvement by the private sector and other Transportation Systems Sector stakeholders is paramount to successfully address these challenges.

Transportation Asset Ownership Impact on R&D. A unique diversity of asset ownership and resultant accountabilities is found in the Transportation Systems Sector, with a large percentage of transportation systems and assets controlled by the private sector, as discussed in section 1. Such diversity of ownership calls for proactive and full engagement with all transportation security partners—Federal agencies; State, local, and tribal authorities; private sector businesses; trade organizations; and other transportation stakeholders—in order to expedite the flow of information and appropriately leverage R&D initiatives throughout the transportation community.

The diversity of the Transportation Systems Sector translates to a wide variety of security and risk management needs that depend on R&D efforts. Table 7-1 provides examples of such needs tied to specific infrastructure elements.

Table 7-1: Sample R&D Security Needs by Transportation Infrastructure Element

Transportation Infrastructure Element	R&D Related Protection Needs
Transportation Infrastructure, Facilities, and Logistical Information Systems	Protecting physical buildings; securing areas, logistics information, and cyber-based systems, including navigation equipment, air traffic control systems, tracking systems, and communication systems needed to support commerce; securing air/train/bus/metro terminals, bridges, tunnels, highways, rail corridors, all transportation surface structures, pipelines, airspace, coastal waterways, port facilities, airports, space launch and re-entry sites; protecting railway and transit stations and facilities, rail yards, bus garages, and rights-of -way for tracks, power, and signal systems.
People	Screening passengers for weapons, chemical, biological, radiological, nuclear, and explosive (CBRNE) substances, and other items considered harmful to other passengers and/or the infrastructure, facilities, or transportation equipment.
Baggage Accompanying Travelers	Screening checked baggage and carry-on baggage to protect against weapons, explosives, CBRNE, and other items considered harmful to other passengers and/or the infrastructure, facilities, or transportation equipment.
Cargo and Parcel	Screening cargo, parcel, or other shipments using transportation assets within the transportation system that stand alone to protect against weapons, explosives, CBRNE, and other items considered harmful to other passengers and/or the infrastructure, facilities, or transportation equipment.
Conveyance Items and Transportation Equipment	Protecting vehicles for surface, water, or air, including airplanes, buses, trains, trucks, boats, and other vehicles that transport people, services, or goods.

The combination of diversity of ownership and wide dispersal of transportation system and asset needs creates a substantial challenge in coordination and planning that must be considered and included in the requirements for transportation R&D programs. Weaving security seamlessly into the fabric of the U.S. transportation network requires closely coupling and integrating R&D advances with security programs. Programs developed must be cost-effective, practical, and able to be integrated into a wide range of operational environments.

For these reasons, the Transportation Systems Sector R&D community must focus on advances in technology that impact practical integration issues at the operational level for achieving security goals while still emphasizing leap-ahead "game-changing" advances through basic (long-term) research.

Inherent Vulnerability of Surface Transportation. The very nature of surface transportation design and operations makes them vulnerable to attack. Surface transportation systems are far more accessible than the commercial passenger aviation system, with multiple entry points, few barriers to access, and with hubs that serve and allow transfers among multiple modes—intercity rail, commuter rail, subway, and bus—and multiple carriers.

Transportation Systems Sector R&D efforts must address the challenges of surface transportation security as laid out in Executive Order 13416, Strengthening Surface Transportation Security. Security technology developed for other purposes must be adapted to the different environment and circumstances of surface transportation. New technologies that are uniquely suited to mass transit and rail systems must be identified and developed.

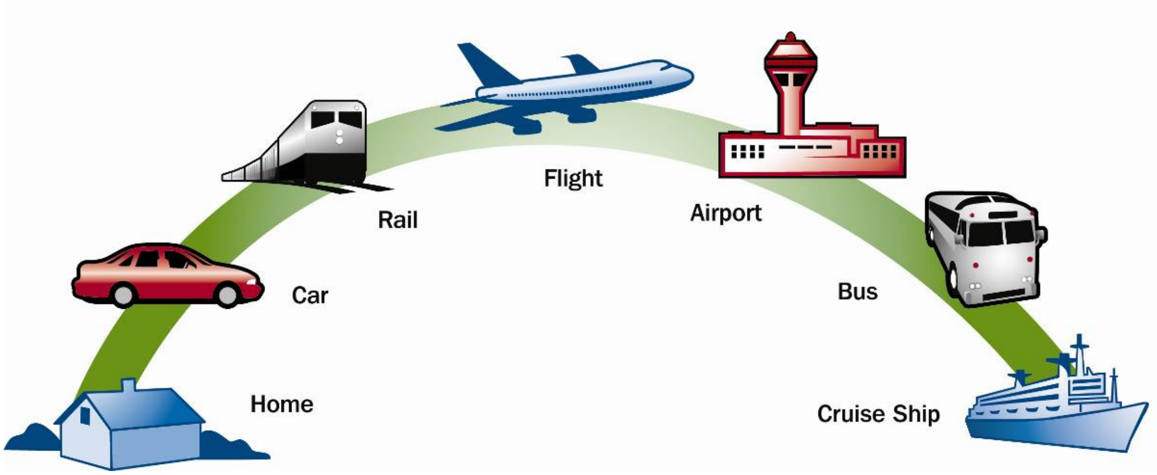
Constant Evolution of Transportation Security. One of the primary characteristics of the transportation security environment is constant evolution. The terrorist threat poses special challenges since terrorists are highly adaptive—seeking to learn and adjust their strategies based on past responses. Terrorists look for ways to defeat or get around current security measures by adapting to changes in security measures.

If a measure of unpredictability is built into operations, terrorists cannot use consistency to their advantage in planning an attack. Security approaches, therefore, must be based on flexibility and unpredictability.

Increasing Dependency on Intermodal Transportation. Driven by the increased mobility of today's society and the expansion of commerce domestically and globally, holistic intermodal security planning across all transportation modes is required. First, similar R&D efforts need to be leveraged across modes. Second, travel or commerce transactions, which span multiple transportation system modes, need analysis, coupled with comprehensive R&D programs, to minimize security exposures during handoffs between transportation modes.

Figure 7-2 illustrates an intermodal passenger transportation example.

Figure 7-2: Intermodal Passenger Transportation Example



International Considerations. The growth in shipment volumes into the United States from foreign ports and borders calls for R&D to solve multiple challenges in such a way that impediments to international commerce are minimized, while safety and security measures are maintained.

The development and implementation of common approaches to CIP and response to cross-border and transnational terrorist incidents is important to the security of America. R&D efforts that support cross-border programs must rely on common definitions, standards, protocols, and approaches in an agreed, coordinated fashion to be effective.

Adjustments to supply chain controls and processes for enhanced cargo flow are in progress. These adjustments include using Known Shipper programs for commercial entities and designated foreign freight companies cleared under the DOD National Industrial Security Program. Developing the use of intelligent targeting systems to identify high-risk cargo and freight and enhanced inspection processes (e.g., using enhanced cargo scanning or an Explosive Detection System (EDS) and Radiation Portal Monitor (RPM)) will address enhanced security initiatives in anticipation of the continually rapid growth of imports into the United States.

7.1.2 Transportation Systems Sector R&D and Technology Community

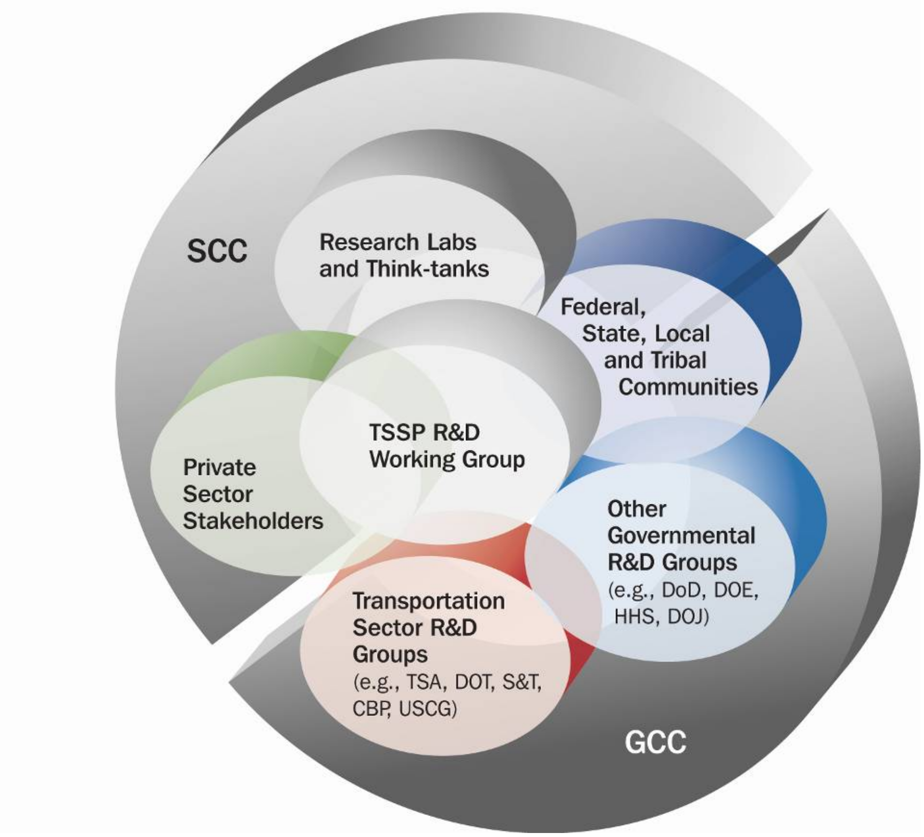
The sector stakeholders contributing to the R&D plan include:

- TSA;
- DHS S&T;
- Other DHS agencies, including USCG, CBP, and G&T;
- Sector-specific agencies, including DOT;
- Other Federal departments and agencies, including OSTP, DOC, USACE, and DoD R&D teams;
- State, local, and tribal DOTs and R&D organizations;
- Private sector owners, operators, and research entities; and
- Academia, **n**ational **l**aboratories, and other **r**esearch **c**enters, including international entities.

7.1.3 Transportation Systems SSP R&D Working Group

Sector-specific planning and coordination are addressed through the GCC and SCC framework. A Transportation Systems SSP Research and Development Working Group (R&DWG) is formulated under these coordinating councils. The group is composed of representatives from the R&D community who are able to articulate long-range vision and requirements for the represented entity, who understand R&D technology capabilities and the inherent value of their potential ability to support that vision, and who have direct influence over the development of requirements and the use of technology within their entity or transportation mode. Figure 7-3 illustrates the Transportation Systems SSP R&DWG.

Figure 7-3: Transportation Systems SSP R&D Working Group


SCC
Research Labs and Think-tanks
Federal, State, Local and Tribal Communities
Private Sector Stakeholders
TSSP R&D Working Group
Other Governmental R&D Groups (e.g., DoD, DOE, HHS, DOJ)
Transportation Sector R&D Groups (e.g., TSA, DOT, S&T, CBP, USCG)
GCC

The role of the Transportation Systems SSP R&DWG is to coordinate and review R&D activities that directly or tangentially affect technologies that support the mission of the NCIP program. The primary mission of the Transportation Systems SSP R&DWG is to improve coordination and prioritization of sector RDT&E efforts and to leverage R&D programs across the stakeholder community.

The Transportation Systems SSP R&DWG will review R&D efforts in place across the Transportation Systems Sector and leverage existing initiatives to strengthen R&D efforts and jointly develop a Transportation Systems Sector R&D Plan. Fostering collaboration and encouraging knowledge sharing will facilitate talent and resource sharing, as will using best practices approaches through lessons learned.

The Transportation Systems SSP R&DWG will use the Transportation Systems Sector GCC and SCC to review the plans and recommendations made on behalf of the R&D transportation communities and may request specific actions from these groups to remove inhibitors or challenges in addressing CI/KR challenges. Special focus will be applied to cross-modal transportation challenges where process, policy, and use of technology intersect. Section 7.4, Transportation Systems Sector R&D Management Process, provides an expanded description of the Transportation Systems SSP R&DWG.

The initial tasks of the Transportation Systems SSP R&DWG listed below are further discussed in section 7.4.1:

- Assimilation of current R&D initiatives;
- Advancing the strategic way forward;
- R&D portfolio assessment; and
- Support for Executive Order 13416, Strengthening Surface Transportation Security**.**

7.1.4 R&D Alignment With Transportation Systems Sector Goals

Drawing from the Transportation Systems Sector goals and the technology-enabling vision of the NCIP R&D Plan, the Transportation Systems Sector R&D Plan will focus on the following strategic objectives:

Table 7-2: Alignment of Sector Goals and R&D Objectives

Transportation Systems Sector Goals	R&D Aligned Strategic Objectives
Prevent and deter acts of terrorism	Develop and deploy state-of-the-art, high-performance, affordable systems to prevent, detect, and mitigate the consequences of CBRNE attacks. Increase awareness of the R&D capabilities available for threat-deterrent actions through stakeholder outreach programs, more timely publication of R&D studies and findings, and more frequent information sharing.
Enhance resilience of the U.S. transportation system	Improve materials and methods to increase the strength and resilience of critical infrastructures for integration into new construction, facility upgrades, and new or upgraded transportation structures (e.g., tunnels, highways, bridges, pipelines, conveyance vehicles, and cargo containers). Architect dynamic, self-learning transportation network systems with tightly defined permissions for secure data access within a common operating picture. Develop layered, adaptive, secure nationwide enterprise architectures to facilitate shared situational awareness to enable real-time alerts to threats at an operational level. Develop equipment, protocols, and training procedures for response to and recovery from CBRNE attacks. Develop methods and capabilities to test and assess threats and vulnerabilities, prevent surprise technology, and anticipate emerging threats.
Improve the cost-effective use of resources	Develop technical standards and establish certified laboratories to evaluate homeland security and emergency responder technologies, and evaluate technologies for SAFETY Act protections. Develop ongoing cross-pollination activities (testing, studies, pilots, etc.) between government and stakeholder partners to expand the pool of available technologies to enhance security. Align Transportation Systems Sector resources and identify a security-relevant transportation R&D portfolio that assists in prioritizing high-need R&D efforts that may include developing common definitions and nomenclatures.

7.2 Transportation Systems Sector R&D Requirements

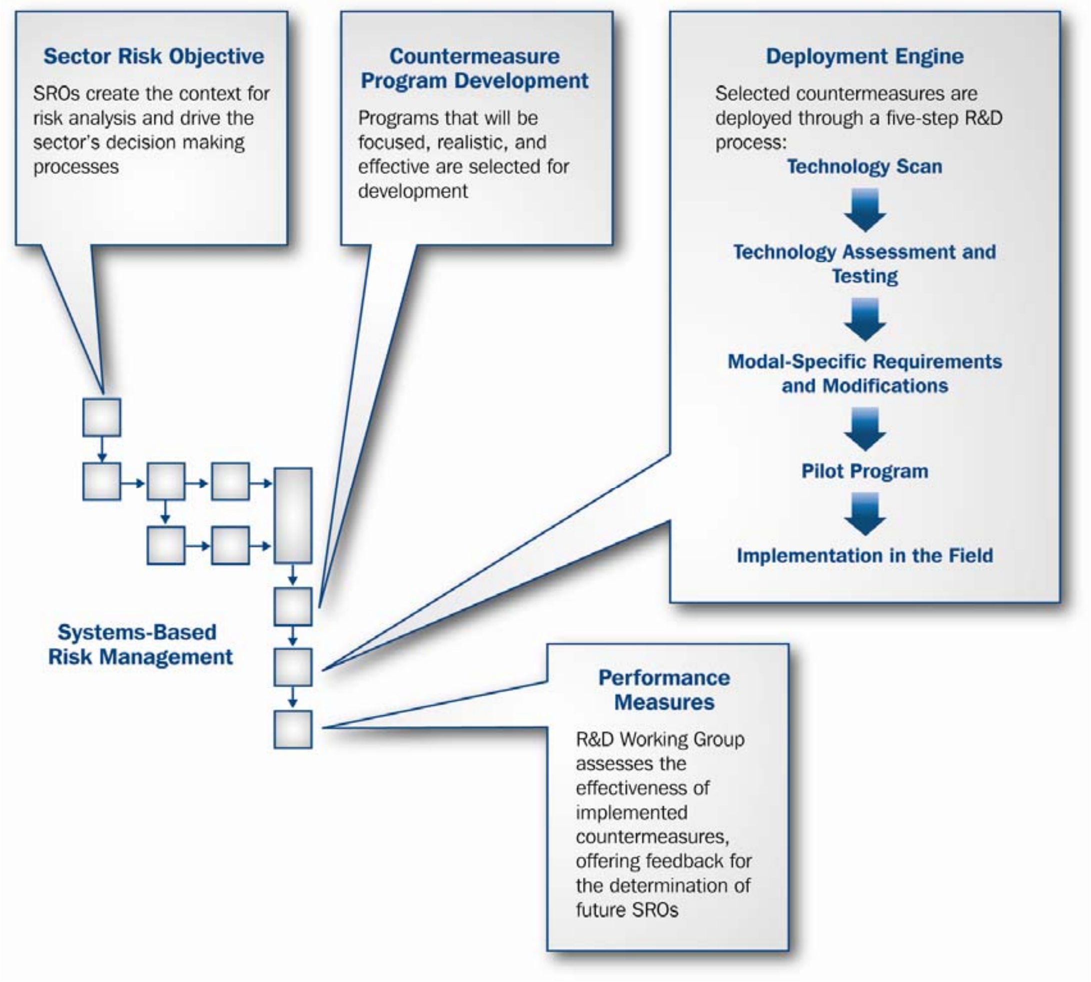
To achieve the Transportation Systems Sector security goals, certain essential capabilities must be obtained through effective R&D, such as:

- Improving existing technology to increase throughput, improve detection, lower false alarm rates, reduce staffing requirements, and improve operational effectiveness;
- Exploring emerging and revolutionary technology as additional security options to protect high-risk transportation assets;
- Developing efficient innovative technology solutions to prevent, protect, detect, respond, and recover;
- Developing security technology solutions to assist in event containment, mitigation of event consequences, and rapid response and recovery;
- Providing guidance on effectively integrating security technology solutions; and
- Creating computer models and algorithms that are interoperable to be accessible to critical infrastructure owners and operators. Also, use common inputs and assumptions.

7.2.1 Process for Defining Transportation Systems Sector Requirements

The risk-based process for identifying R&D requirements to develop these capabilities is illustrated in figure 7-4.

Figure 7-4: Sector-Wide R&D Risk-Driven Requirements Model


Sector Risk Objective
SROs create the context for risk analysis and drive the sector's decision making processes
Countermeasure Program Development
Programs that will be focused, realistic, and effective are selected for development
Deployment Engine
Selected countermeasures are deployed through a five-step R&D process:
Technology Scan
Technology Assessment and Testing
Modal-Specific Requirements and Modifications
Pilot Program
Implementation in the Field
Systems-Based Risk Management
Performance Measures
R&D Working Group assesses the effectiveness of implemented countermeasures, offering feedback for the determination of future SROs

The SBRM framework described in sections 3, 4, and 5 will be used to identify and prioritize critical transportation systems and assets. Once the risks are identified, the areas of concern will be verified with appropriate government and stakeholder participants.

Risk mitigation options, including physical, process, and institutional changes, will be considered for these systems and assets. Assessing the options based on the alignment with sector security goals, NCIP R&D technology-enabling goals, and other guidance from sector stakeholders provides a prioritization of the mitigation options.

Under the leadership of TSA and the Transportation Systems Sector GCC and SCC partners, the Transportation Systems SSP R&DWG will enable collaboration across all stakeholders to identify the R&D-related capabilities that the sector currently has that could be used to mitigate any identified risks.

R&D efforts are derived using a technology-scan approach of available options to be considered, including current best practices. From these efforts, development programs are derived and often include identifying short-, medium-, and long-term desired outcomes. If approved, the path results in either a basic, applied, or development research program, or some combination thereof. These programs may then result in pilot test programs in the appropriate laboratories, followed by field testing and potential deployment.

Since Transportation Systems Sector R&D is a shared activity across the Federal Government and private sector, a great deal of insight is harnessed to help develop the appropriate technology requirements. Many of these requirements will be addressed through normal planning and programming activities.

Additional requirements that address intermodal transportation or exceed an individual stakeholder's ability to deliver must be collectively approached by the sector. Such requirements will be identified through the Transportation Systems SSP R&DWG outreach plans with other planning initiatives.

If the capability does not currently exist, the R&DWG will either take the lead in examining other programs that may be adapted to address the need or direct new R&D activities through the grants process or other funding vehicles to encourage new design capabilities.

R&D inputs to requirements are also driven by the evolution of technology capabilities. The continual scanning for new technology advances across the government, private sector, and academia enables greater potential deployment of technology-enabled solutions for enhanced security at the same or less cost than existing protection measures. It also reveals the potential for new security capabilities not previously considered.

7.2.2 Baseline Transportation Systems Sector Requirements

Examples of sector requirements derived from the SBRM process include:

1. **Enhance screening effectiveness for passengers, baggage, and cargo for all surface, maritime, and air transportation modes:**
   - Incorporate screening for CBRNE;
   - Increase throughput, improve detection, lower false alarm rates, reduce staffing requirements, improve operational effectiveness, and provide cross-modal capability**;**

- Exploit recent advances in biotechnology to develop novel detection systems and broad spectrum treatments to counter the threat of engineered biological weapons;
- Develop transformational capabilities for stand-off detection of special nuclear material and conventional explosives; and
- Explore emerging and revolutionary technology to improve current screening and detect emerging threats.

2. **Enhance infrastructure and conveyance security:**
    - Improve detection and deterrence, including integration of biometric-based systems;
    - Incorporate "security by design" into infrastructure and systems. Develop design guidance and risk mitigation strategies to integrate into infrastructure and facilities;
    - Develop improved materials and methods to increase resilience of infrastructure;
    - Improve and enhance container and vehicle tracking;
    - Provide secure authentication and access control;
    - Develop quick and cost-effective sampling and decontamination methodologies and tools for remediation of biological and chemical incidents;
    - Explore biometric recognition of individuals for border security and homeland security purposes in a rapid, interoperable, and privacy-protective manner; and
    - Recognize and expedite safe cargo entering the country legally, while securing the borders against other entries.
3. **Improve information gathering and analysis:**
    - Provide an integrated view of available incident information;
    - Increase domain awareness by providing dynamic situational awareness and analysis;
    - Develop risk analysis and situation simulation models for assessing and evaluating mitigation and response/recovery strategies; and
    - Develop integrated predictive modeling capability for chemical, radiological, or nuclear incidents, and collect data to support these models.
4. **Provide a common operating picture for transportation systems:**
    - Develop adaptive, self-healing, secure, and interoperable enterprise architectures;
    - Incorporate resiliency into networks and systems; and
    - Establish data standards that facilitate a common operating picture.

7.2.3 Prioritization of Transportation Systems Sector R&D Requirements

Multiple criteria will be used to prioritize Transportation Systems Sector security requirements and assess the portfolio of new and existing initiatives. Consistent with OMB performance assessment tools and other best practices, the measures include:

- Relevance, such as correspondence with strategic goals, magnitude of strategic gap coverage, and level of risk mitigation;

- Compatibility with current operational environment;
- Cross-modal capability and potential;
- Quality of design;
- Performance, such as output and outcome measures, schedules, and decision points; and
- Time to complete or pilot-ready status.

New perspectives may be brought by the Transportation Systems SSP R&DWG to the course of an "in-development" program (e.g., insights on relevance, possible expansion or modifications, or other assistance).

7.3 Transportation Systems Sector R&D Plan

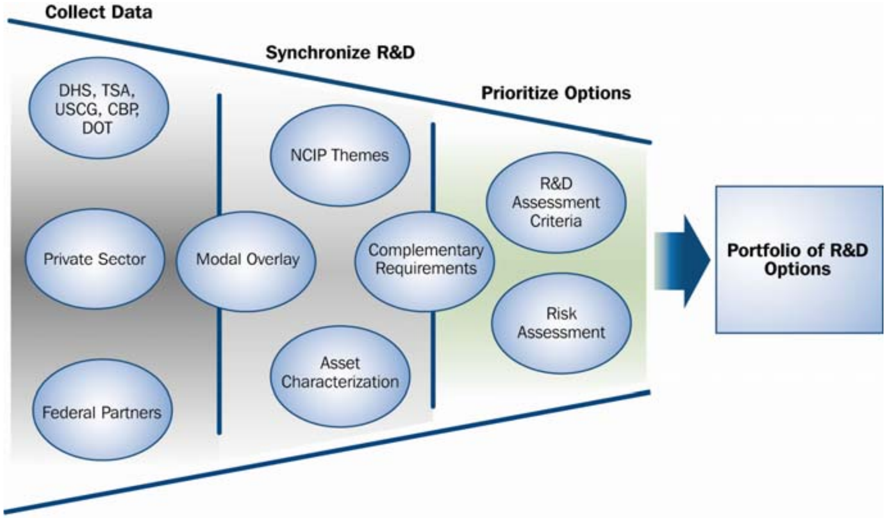
R&D in the Transportation Systems Sector will focus on advances in science and on the logical and practical integration issues at the operational and human performance level concurrently and rapidly, for achieving sector security goals. The mechanism for planning this integration and execution is the Transportation Systems Sector R&D Plan.

7.3.1 Components of the Transportation Systems Sector R&D Plan

The R&D Plan has two primary parts. The first part is reflective of the efforts undertaken by the sector to meet the sector goals. It describes the portfolio of existing initiatives that are designed to respond to specific requirements within the sector. This includes the Federal R&D community and R&D programs from the States and private industry related to the CIP. The second part of the plan takes a prospective view of the portfolio, focusing on new initiatives that meet the emerging and ongoing requirements of the sector.

Figure 7-5 illustrates the process for developing the R&D Plan.

Figure 7-5: Transportation Systems Sector R&D Plan Process



7.3.2 Sources of Input to the Transportation Systems Sector R&D Plan

To produce the Transportation Systems Sector R&D Plan, an initial review of transportation security R&D programs was conducted. Sources for this preliminary review included:

- TSA
- DOT
- CBP
- USCG
- OSTP
- DHS S&T
- National Science Foundation (NSF)
- DOD
- Other Federal R&D
- Miscellaneous sources

Plans are being developed to incorporate R&D programs from academia; the private sector; and other Federal, State, local, and tribal governmental entities to complete the data collection stage of the process.

7.3.3 R&D Portfolio Framework

A preliminary Transportation R&D Portfolio aggregates ongoing R&D efforts by the six individual modes of transportation: Aviation, Maritime, Mass Transit, Highway, Freight Rail, and Pipeline. One consolidated portfolio of programs relevant to intermodal transportation issues has been developed from the initial review of programs.

One of the more perplexing challenges is establishing a common baseline. Without common nomenclatures, definitions, or simple clarification of what is considered an R&D activity in one agency versus another, the ability to assimilate R&D initiatives for comparison purposes is potentially prone to misrepresentation. Once a common baseline is established, comparisons and groupings can be accumulated in a logical way.

A proposed matrix framework that maps the nine NCIP technology-centric R&D themes with a sector-specific asset categorization that recognizes the unique characteristics and requirements of transportation security will provide an advance toward developing a baseline for the Transportation Systems Sector R&D programs. This framework aligns the types of technology applicable to homeland security with the transportation system assets (infrastructures and components).

The NCIP R&D Plan is structured around themes that support all 17 critical infrastructure sectors. The nine themes were based on the repeated appearance in the concerns of infrastructure owners and operators, industry representatives, and government officials. Overlaying this theme-based structural model with people (passengers and employees), goods (baggage and cargo), conveyance, infrastructure, and facilities helps to create a logical framework from which to begin to assess the Transportation R&D Portfolio. The layered framework helps to identify complementary initiatives, duplications, and strategic gaps in existing and planned R&D efforts for the sector.

The framework will provide a common language and reference point that allows the comparison of R&D programs and will enable formulation of a strategic way forward. The framework does not attempt to dictate individual agency budget considerations or requirements.

Current Federal transportation security R&D initiatives have been mapped against the nine NCIP themes and associated sub-themes as a first step toward developing the baseline R&D Portfolio. Particular emphasis was placed on identifying cross-modal programs for the sector.

The Transportation Systems SSP R&DWG will continue the process of assessing all stakeholders' current and planned R&D initiatives against the NCIP themes to assist in identifying research strategic gaps and requirements.

Once the data collection is completed and final framework charts are established and agreed upon, the Transportation Systems SSP R&DWG can develop summary conclusions about Transportation Systems Sector R&D programs, including:

- Strengths and goal coverage;
- Cross-modal capabilities and potentialities;
- Complementariness and interdependence of programs; and
- Opportunities for collaboration.

Completing the data collection and framework charts can help fulfill the requirements for Executive Order 13416, Strengthening Surface Transportation Security. This work will be conducted on an ongoing basis as part of the Transportation Systems SSP R&DWG activities.

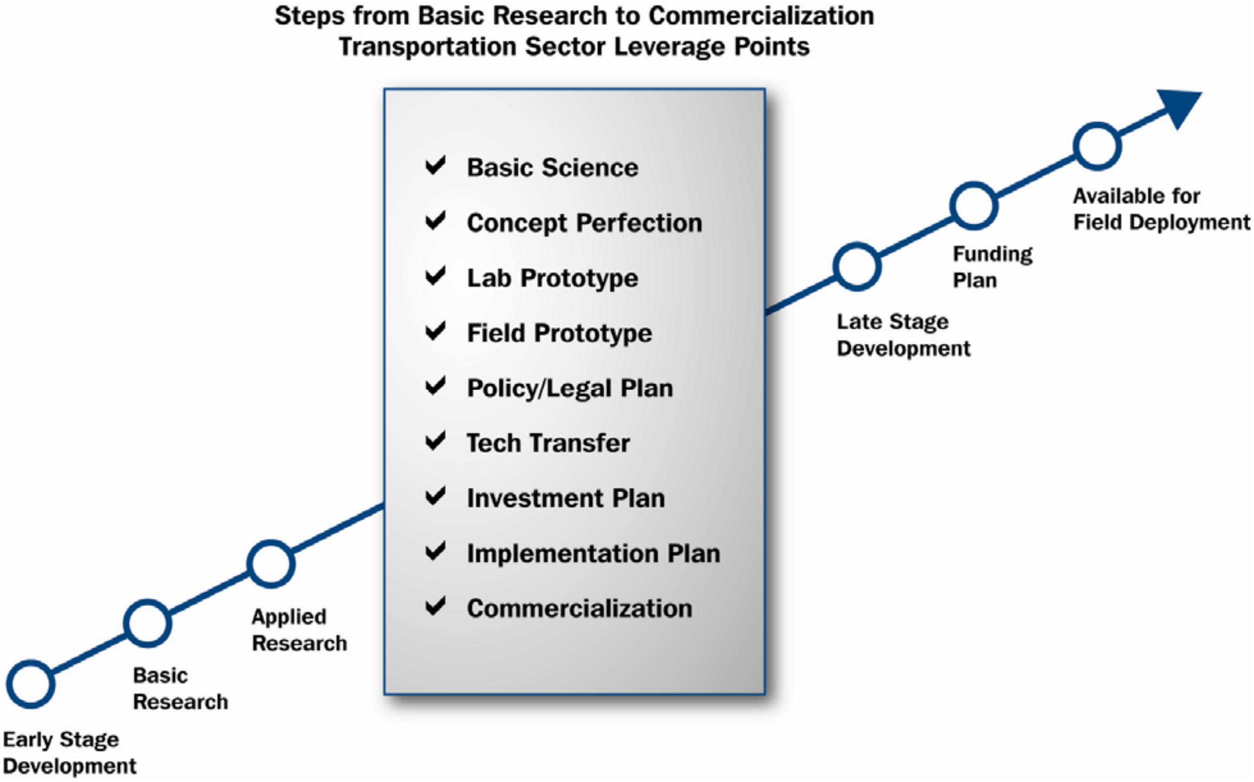
7.3.4 Technology Transition Through the R&D Life Cycle

All phases of research are required to bring potential technologies to bear for any given security challenge. The Transportation Systems Sector looks to the national laboratories and academia for basic research. The DHS S&T is utilizing the expertise of nine national laboratories under Section 309 of the Homeland Security Act of 2002 (Public Law 107-296). Academia has been directly engaged through a number of activities, ranging from the funding of university-based research centers, such as the DHS S&T Centers of Excellence and Cooperative Centers and DOT's University Transportation Centers (UTC), to direct funding of specific research programs, such as TSA-funded nanotechnology research at the University of North Carolina at Chapel Hill.

Applied research and early stage pilot test and development activities are the primary nature of transportation R&D activities by the transportation agencies and the private sector. Applied research is necessary to bring concepts to a level of maturity necessary to transition to the development of a full-fledged set of products or processes. Funding and/or support from the government or private sector is necessary beyond this point to bring products to a commercially viable state.

The steps to bring to bear relevant technology capabilities into the field extend from the identification of basic research to eventual commercialization of a product. While each technology may require a different path to operationalization due to the uniqueness of the technology and the specific requirements of the transportation modes, a high-level process of leverage points within the R&D cycle for the Transportation Systems Sector is illustrated in figure 7-6.

Figure 7-6: Steps From Basic Research to Commercialization



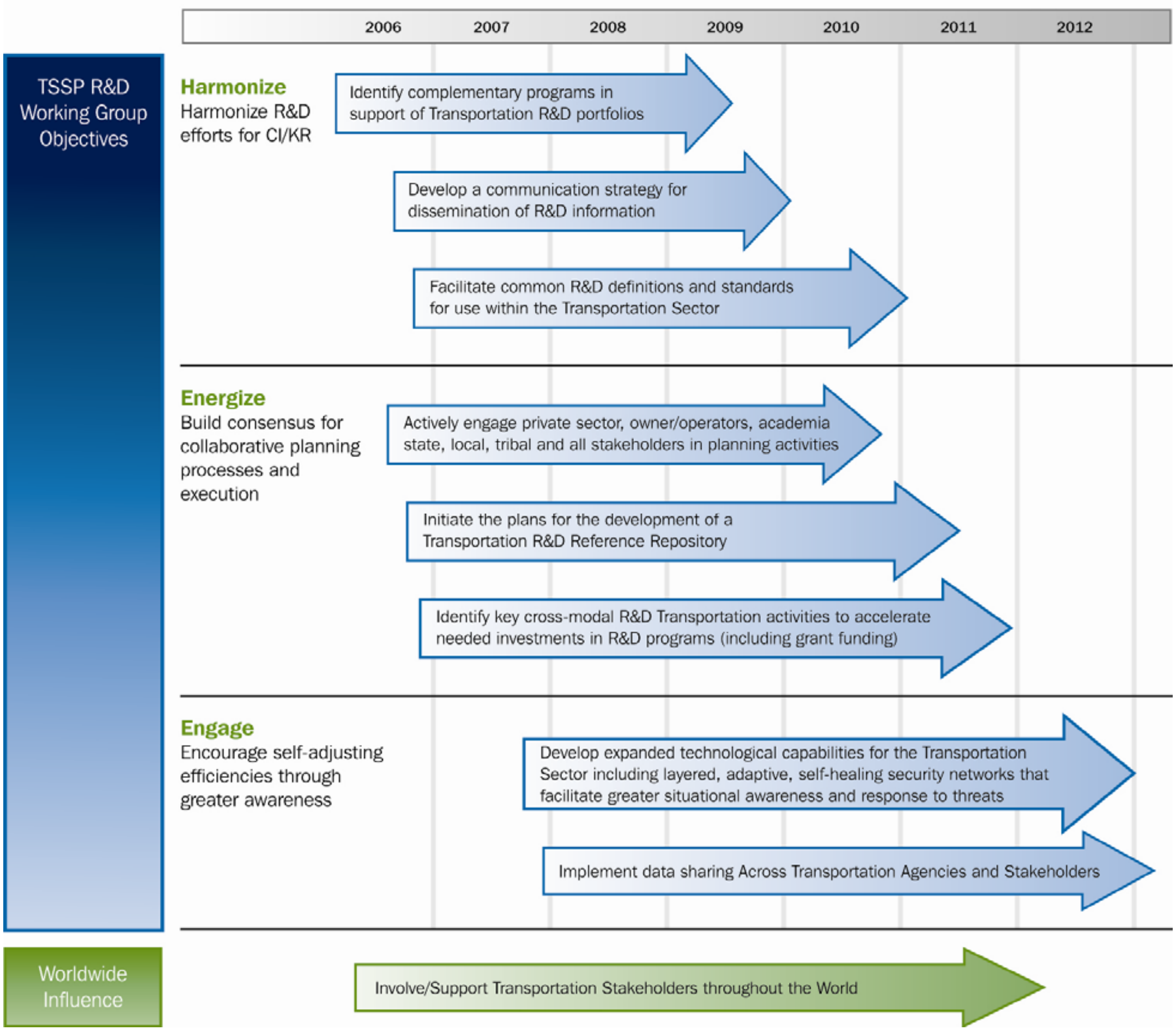
The Transportation Systems SSP R&DWG will work with the core governmental agencies, the DHS S&T, and private sector stakeholders to identify the appropriate process for leveraging common and cross-sector R&D initiatives to accelerate R&D developments where the greatest risks lie. As part of the portfolio development activities and identifying ways forward, the Transportation Systems SSP R&DWG, in partnership with private sector stakeholders and participating governmental agencies, will refine the development of more efficient processes to better leverage cross-organizational efforts, resources, and investments within the R&D and deployment cycles.

7.3.5 Transportation Systems Sector R&D Way Forward

Coordinating applied R&D initiatives across the transportation modes for increased security will require collaboration with the Federal, State, local, and tribal governments; the science community; the private sector; and the public at large. Eliminating Territorial boundaries of responsibility for achieving the greater purpose will take precedence in planning activities, whether governmental or private concerns. Understanding and accepting the risks, trade-offs, and priorities for increased security measures and contingency planning are the responsibility of all stakeholders in the Transportation Systems Sector.

Figure 7-7 highlights key planning objectives and milestones to be achieved in the next 5 years, including identifying technologies currently available to both government and private industry for immediate use. The creation of a technology clearinghouse, currently underway, is captured in the "Harmonize" section of the figure.

Figure 7-7: Transportation R&D Way Forward


2006
2007
2008
2009
2010
2011
2012
TSSP R&D Working Group Objectives
Harmonize
Harmonize R&D efforts for CI/KR
Identify complementary programs in support of Transportation R&D portfolios
Develop a communication strategy for dissemination of R&D information
Facilitate common R&D definitions and standards for use within the Transportation Sector
Energize
Build consensus for collaborative planning processes and execution
Actively engage private sector, owner/operators, academia state, local, tribal and all stakeholders in planning activities
Initiate the plans for the development of a Transportation R&D Reference Repository
Identify key cross-modal R&D Transportation activities to accelerate needed investments in R&D programs (including grant funding)
Engage
Encourage self-adjusting efficiencies through greater awareness
Develop expanded technological capabilities for the Transportation Sector including layered, adaptive, self-healing security networks that facilitate greater situational awareness and response to threats
Implement data sharing Across Transportation Agencies and Stakeholders
Worldwide Influence
Involve/Support Transportation Stakeholders throughout the World

7.4 Transportation Systems Sector R&D Management Process

7.4.1 Sector R&D Governance

The Transportation Systems SSP R&DWG is composed of members from core transportation stakeholders (see section 7.1.3) with the primary mission to improve coordination and prioritization of sector RDT&E efforts and to leverage R&D programs across the stakeholder community.

The strategic objectives of the R&DWG are to:

- Harmonize transportation R&D efforts for CI/KR by identifying currently available technology and complementary programs, facilitating common definitions and standards, and disseminating best practices;
- Build consensus for collaborative planning processes and execution with all sector stakeholders; and

- Engage and encourage efficiencies in sector R&D through greater awareness and communication by implementing data sharing across sector agencies and stakeholders.

The Transportation Systems SSP R&DWG will be supported by the Transportation Systems Sector GCC and SCC. The R&DWG will use these councils to review the plans and recommendations and, if needed, assist in removing inhibitors in addressing CI/KR challenges.

Membership is initially comprised of core government, national laboratories, and academic representatives, with the private sector engaged through the Transportation Systems SCC. Plans are being developed to fully integrate the private sector into the R&DWG.

The R&DWG will determine the scope of continuing management and processes for the group, such as objectives; primary and secondary participation composition; and operational guidelines, such as the time commitments required for participants from sponsoring agencies and rules of engagement.

The initial tasks of the Transportation Systems SSP R&DWG in partnership with the broader transportation R&D communities include facilitation of the following.

Inventory and Assessment of Current R&D Initiatives

- Identify complementary technology requirements;
- Identify research strategic gaps;
- Publish non-confidential results of pilot tests within the Transportation Systems Sector;
- Identify cross-modal prioritization parameters; and
- Promote understanding of the use of infrastructure protection security grants to assist in implementing security requirements and guidelines for R&D transportation efforts.

Strategic Way Forward

- Actively engage private sector; academia; and State, local, and tribal agencies in planning activities;
- Facilitate and coordinate R&D planning activities across all sector modes; and
- Identify key cross-modal activities to accelerate investments in transportation R&D with a focus on risk-based needs.

R&D Portfolio Assessment

- Facilitate development of a common terminology and approach to characterize stages of R&D activities to improve technology transition; long- and short-term R&D requirements development for enhanced portfolio quality, including technology-scanning methods; and system vulnerabilities and transportation mode R&D priorities; and
- Develop and apply criteria to ensure that the current and planned R&D portfolio meets the future needs of the Transportation Systems Sector.

Support for Executive Order 13416, Strengthening Surface Transportation Security

- Maintain a list of current R&D initiatives that meet or have the potential to meet sector CI/KR protection challenges; and
- Facilitate the development of standards that meet transportation security CI/KR application needs, including surface transportation.

Future focus areas for the working group include:

- Coordinate community-level cross-sector and cross-agency proof-of-concept R&D pilot initiatives;
- Develop technology-scanning approaches to find and accelerate applicable security innovation from R&D within the private sector;
- Develop expanded technological capabilities that address intermodal and surface transportation challenges;
- Facilitate standards identification development;
- Coordinate communication strategy for dissemination of best practices, including development processes; and
- Establish community outreach to the transportation R&D community and transportation stakeholders.

The Transportation Systems SSP R&DWG will meet monthly to review portfolio characterization efforts and provide recommendations, inputs, and plans, including the annual update of the Transportation Systems SSP, and coordinate with the overall R&D programs in development with the varying stakeholders.

Within the Transportation Systems Sector, many R&D activities and entities have responsibility for cross-community coordination roles. Leadership engagement should be focused on optimizing the efforts of these entities for more effective and efficient R&D across the whole sector.

7.4.2 Coordination With Other Planning Efforts

The Transportation Systems SSP R&DWG will work to provide input and guidance to the developers of the NCIP R&D Plan and other R&D government transportation security planning efforts and Executive Orders related to CI/KR, such as Executive Order 13416, Strengthening Surface Transportation Security, as they arise. The Transportation Systems SSP R&DWG will devise a set of principles and working methods for coordinating strategic planning activities among the contributing agencies and stakeholders.

The Transportation Systems SSP R&DWG will establish outreach plans with other planning initiatives. Examples of these are HSPD initiatives, the joint TSA and DOT Executive Steering Committee (ESC), and the Next Generation Airspace Transportation System's Joint Planning Development Office (NGATS/JPDO). Through the efforts of the Transportation Systems SSP R&DWG, the need for Transportation Systems Sector reporting will be aggregated, streamlining government and other similar reporting efforts required over time.

7.4.3 Importance of Private Sector Involvement

When fully established, the Transportation Systems SSP R&DWG will include the private sector and other nongovernmental group members involved in the Transportation Systems Sector or R&D community to collaborate in developing the Transportation Systems SSP R&DWG charter and deliverables. The goal of private sector involvement is to ensure stakeholder participation to achieve commonly defined protection goals and to foster collaboration that accelerates R&D capabilities to more rapidly satisfy sector requirements. There are numerous private industry entities that contribute to security research. For example, the freight rail industry conducts extensive research in the areas of safety, security, and efficiency at the Transportation Technology Center in Pueblo, Colorado. The goal of the R&DWG is to add private sector members to the team by first quarter of 2007.

The R&DWG is also establishing community outreach plans for State, local, tribal, and private sector entities to support more timely exchange of transportation security information. Improving the understanding of needs and requirements in the field by direct involvement and participation with local community efforts will improve the quality of R&D efforts and efficiencies. Future plans from these outreach efforts include reducing security risks by virtue of better coordination and identifying high-value potential pilot R&D programs that foster collaboration between local government and agencies and between the private sector and citizens.

Equally responsible, the private sector has a critical role in implementing transportation security initiatives because of its ownership of a significant percentage of transportation assets. The R&DWG recognizes that security initiatives developed by the government must be closely coupled with the operational goals and requirements of the private sector to be effective.

In addressing the rapid evolution of terrorist threats, including the potential of advanced weaponry in the hands of terrorists with clear intent to harm, the Transportation Systems Sector R&D community does not have the luxury of developing pure science removed from its context. Rather, in partnership with government and private sector teams, R&D initiatives can be quickly, safely, and cost-efficiently integrated into operational environments in parallel with game-changing research aimed at new and emerging threats. Keeping our communities safe under threat of attack will require community accountability and a heightened state of awareness between stakeholders and the transportation R&D community to effectively identify and mitigate risks and deter or respond to threats.

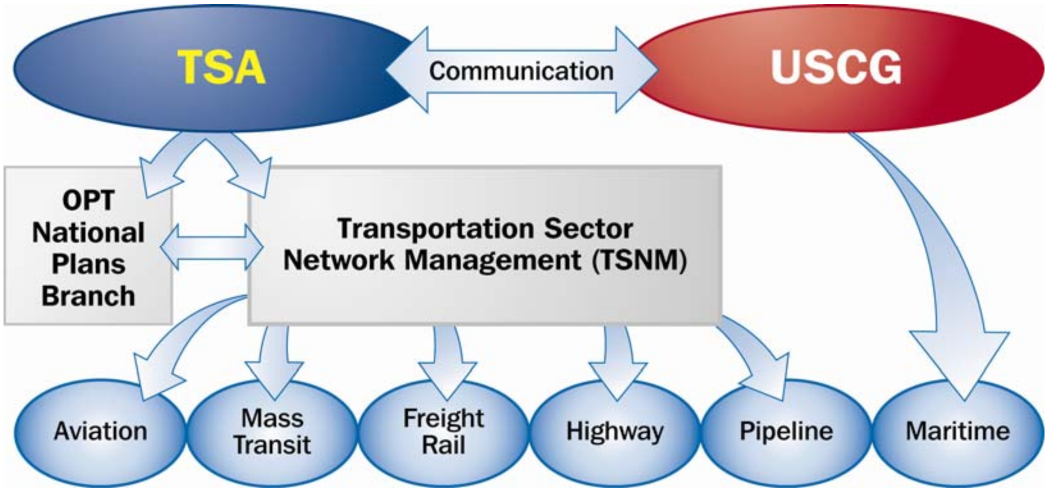
8. Manage and Coordinate SSA Responsibilities

This section describes the management process for supporting all NIPP-related responsibilities and how these responsibilities will be achieved. Additionally, this section outlines the NIPP information-sharing mechanisms that the Transportation Systems Sector uses, and details the processes, programs, and tools in place to ensure protection of the CI/KR information collected.

8.1 Program Management Approach

TSA, as the Transportation Systems Sector SSA, created a National Plans Coordination Branch, a new division under the Office of Operational Process and Technology (OPT), RMSP Division. The primary responsibility of the division is to align national strategic planning efforts such as the NIPP. Through this division, all TSA SSA responsibilities outlined in the NIPP will be performed and executed. The SSA is also responsible for the program management function of developing, updating, and implementing the Transportation Systems SSP in coordination with all security partners through the GCC/SCC framework. This approach is further depicted in figure 8-1. The USCG, as the SSA for the maritime transportation mode and as the chair of the Maritime Modal GCC, will continue to work cooperatively and collaboratively with the TSA; CBP; and other Federal, State, local, and tribal agencies. The Maritime Modal GCC will work with industry security partners to implement the NIPP requirements of CI/KR protection—to help prevent, prepare for, protect against, respond to, and recover from terrorist attacks, natural disasters, and other emergencies.[21] TSA also has responsibilities for coordinating and executing sector security strategies.

Figure 8-1: Transportation Sector Network Management Structure



8.1.1 Transportation Sector Network Management

Based on the Secretary of Homeland Security's Second Stage Review (2SR) initiative and the vision TSA leadership holds, TSA adopted an organizational structure arranged along mode-specific lines. Each modal GCC, chaired by a Transportation Sector Network Management (TSNM) general manager, will focus on implementing transportation security planning efforts and coordinating key

[21] The NIPP and the NRP together provide a comprehensive, integrated approach to the homeland security mission (NIPP, June 2006, p. 6).

industry and stakeholder functions, such as modal implementation plans. The benefits of this structure are:

- Effective communication and coordination with industry stakeholder entities to collaboratively address security needs important to the sector, such as sharing robust risk, intelligence, and threat information;
- A coordinated and focused approach for addressing private sector security initiatives and activities through the NIPP SPM that will lead to effective policy and security decisions for all modes of transportation; and
- Enhanced information-sharing protocols through the GCC and SCC and other mechanisms to ensure timely and data-driven planning and decisionmaking.

Using the GCC/SCC structure, the SSAs will work with transportation security partners to ensure that effective program management and communications tools are in place to accomplish the future milestones described in section 6.

8.2 Processes and Responsibilities

8.2.1 SSP Maintenance and Update

The Transportation Systems SSP is an evolving document and, as such, it needs to be maintained and updated based on significant events, changes in the sector's security posture, or changes to the sector's approach to securing the sector. Because the Transportation Systems Sector is inherently complex in organizing around CI/KR protection efforts, the Transportation Systems SSP is a 3- to 5-year strategic planning document collaboratively developed using the GCC/SCC framework. Since the December 2006 version of the Transportation Systems SSP will be the sector's initial step in delineating a revised approach to augmenting the sector's CI/KR protection efforts, the Transportation Systems SSP will undergo periodic updates. This process can align with the NIPP triennial update cycle once the sector's leadership framework (Transportation Systems Sector GCC and Transportation Systems SCC) determines that the Transportation Systems SSP fully reflects and encompasses the sector's refinements in an SBRM approach; aligns resources to targeted programs and initiatives; measures the effectiveness of security programs, actions, and initiatives; and establishes a sector-wide R&D and information-sharing approach.

8.2.2 Resources and Budgets

As the SSAs, TSA and USCG, working with the GCC/SCC framework, will outline their respective CI/KR protective requirements and related budgeting information as part of the OMB/Federal budgeting process outlined in the NIPP through the sector CI/KR Protection Annual Report. TSA will initiate appropriate information-gathering efforts with all security partners during the February-to-June timeframe of each fiscal year to assist in the preparation of the annual report. The process for determining important and relevant CI/KR programs will include appropriate consideration of information provided by the transportation security partners, based on SROs, cost-effectiveness, and value to the overall sector's security needs. This sector-wide analysis will inform and facilitate determinations regarding which security programs merit consideration to target for funding through the OMB budgeting cycle.

Additionally, the USCG, as the SSA for the Maritime Mode, will work within its own budget models to provide justifications and execution plans for its security programs. As a multi-mission service, the USCG's assets are used to meet requirements from across its 11 federally mandated mission programs, one or more of which may contribute to CI/KR protection. The USCG does not have a program dedicated to CI/KR protection, but is able to extrapolate and infer degrees of effort that contribute to infrastructure protection, and will use such methods in its approach to CI/KR risk management.

As previously mentioned, the sector-wide analysis is in no way intended to remove the budgetary discretion of individual agencies in submitting budget requests. Among agencies across the sector, determinations on which security programs merit consideration for additional funding shall be advisory only in nature.

8.2.3 Training and Education

The Transportation Systems SSP SBRM framework cannot be accomplished without robust training and continuous education to expand and augment organizational and individual CI/KR protection expertise.

Transportation Systems Sector security partners would greatly benefit from continued training and education on many security-related areas, such as risk evaluation and assessments, response and recovery, and other CI/KR security-related topics. An example course is the CI/KR Protection Qualification Course/Curriculum for Federal employees. The course will be available to all Federal employees whose CI/KR job performance involves at least 50 percent of their duties in analysis or assessment. This certified baseline training course offers agencies a standard for assessing CI/KR. To attend the course, students are required to complete a list of prerequisites and submit online learning certificates of completion. The course outline includes, among other topics:

- NIPP and CIP Overview;
- Risk Management Concept;
- Cyber, Physical, and National Security;
- Operations Security (OPSEC);
- Interdependencies (three key infrastructure interdependencies: water, electric, and power); and
- Grants Process (BZPP).

8.3 Implementing the Sector Partnership Model

As described in section 1 and further addressed in the modal implementation plans, the NIPP SPM is strongly advocated throughout the Transportation Systems SSP and the modal implementation plans as a collaborative mechanism for government and private industry to work together in protecting the Nation's critical infrastructure. Through this collaborative framework, both government and private industry security partners will facilitate cross-cutting planning, policy setting, coordination, and information sharing to determine the most cost-effective, efficient, and targeted approach for developing and implementing security programs based on a risk management framework.

8.3.1 Coordinating Structures

The Transportation Systems Sector established its GCC in January 2006. Since the sector functions by mode, the Transportation Systems Sector GCC is further segmented and organized by modal GCCs (Aviation, Maritime, Mass Transit, Highway, Freight Rail, and Pipeline), as well as by modal SCCs. The primary objective of the Transportation Systems Sector GCC and the forthcoming Transportation Systems SCC is to provide effective coordination for transportation strategies, initiatives, policies, and information sharing between the Federal Government, private industry, sector, and other security partners. The modal implementation plans are separate annexes to the Transportation Systems SSP, allowing modal GCCs and SCCs to develop specific plans to address how each mode will achieve the sector goals.

8.4 Information Sharing and Protection

As described earlier in this plan and detailed further in the modal implementation plans, a necessary component of the SPM is information sharing. The sharing of important and relevant security information between Federal, State, local, and tribal governments must occur frequently. While the sector's GCC/SCC framework is an effective way for government and private sector representatives to communicate and coordinate efforts, additional mechanisms are available that foster good communication and information sharing. The DHS has established several information-sharing platforms to disseminate and receive information.

Homeland Security Information Network. HSIN is a highly secure network backbone built over the Internet with a common set of information-sharing functions and tools for various private sector communities with common security interests. This network, in particular the portal for CIP called Critical Sectors (HSIN-CS), is a suite of tools that sector councils can use for information sharing, coordination, and communication about alerts, incidents, and planning efforts within the sector. This supports the exchange of threat information to critical infrastructure owners and operators in a variety of industries and locations, first-responders, and local officials.

Information Sharing and Analysis Centers (ISACs). ISACs exist within the Transportation Systems Sector, including mass transit, surface transportation (freight rail), highway, and maritime. Sector councils are not intended to replace the information-sharing functions provided by the ISACs. For those sectors that had established ISACs prior to the development of the NIPP, the sectors may continue to rely on them for operational and tactical capabilities for information sharing, such as threat alerts, and, in some cases, support for incident response activities.

The information-sharing process within each mode is further described in the modal annexes.

To facilitate the mandates of the Aviation and Transportation Security Act (ATSA), TSA has operationally coordinated and worked with transportation industry ISACs daily. Various ISACs have access to and work with the Transportation Security Operations Center (TSOC) and with TSA's modal experts and intelligence personnel. ISAC personnel have access to information and intelligence consistent with security policies. Working with ISACs supports the following ATSA requirements:

- TSA receives, assesses, and distributes intelligence information related to transportation security;
- TSA assesses threats to transportation;

- TSA serves as the primary liaison for transportation security to the intelligence and law enforcement communities;
- TSA coordinates countermeasures with appropriate departments; and
- TSA manages and provides operational guidance to field security resources daily.

In addition, ATSA tasks TSA with data sharing, correlating and safeguarding data, and performing a cooperative analysis to identify and effectively respond to threats to transportation security. The goals of continued daily, operational ISAC coordination are to continue:

- Improving methods of receiving information from transportation and transportation-related industries through ISACs, as well as coordinating and sharing information and intelligence with the industry;
- Seeking transportation and transportation-related industry participation in ISACs;
- Meeting quarterly with intelligence analysts (ISAC analysts) to review threat level; and
- Providing transportation and transportation-related ISACs access to the TSOC and to appropriate information and intelligence related to the security of the transportation industries.

Homeport. Homeport is the USCG's newest tool for providing information and service to the public over the Internet. It is an enterprise Internet portal that combines secure information dissemination, advanced collaboration, and provides a public-facing interface for internal USCG processes. In its first release, Homeport supports secure information sharing. Homeport version 1.0 provides information dissemination and collaboration for Area Maritime Security Committees (AMSCs), as well as e-mail notification capabilities. The public can access information related to Marine Safety, Security, and Environmental Protection missions, including, but not limited to, regulations, policy, publications, and forms. Homeport version 1.0 supports several different types of end users, including the general public, vessel and facility security officers, USCG personnel, and maritime committee members.

Area Maritime Security Committees. USCG sponsors an AMSC for each USCG Captain of the Port zone. The AMSCs, under the direction of a Federal Maritime Security Coordinator (FMSC), are a cornerstone of U.S. national maritime security, coordinating and collaborating with various Federal, State, and local authorities and private sector maritime stakeholders toward enhancing and maintaining port security. The AMSCs have already played an integral role in developing the various Area Maritime Security Plans required under the Maritime Transportation Security Act (MTSA). Additionally, the AMSC provides advice on identifying critical port infrastructure and operations, determines mitigation strategies and implementation methods, develops and describes processes for continuous evaluations of overall port security, serves as a link for communicating threats and changes in Maritime Security (MARSEC) levels, and disseminates appropriate security information to port stakeholders.

Critical Infrastructure Warning Information Network. This private government network is within HSIN and provides mission-critical connectivity and a survivable DHS capability for information sharing, collaboration, and alerting Federal, State, and local agencies on critical infrastructure restoration when primary forms of communication to the agencies are unavailable.

Appendix 1: List of Acronyms and Abbreviations

AAR	Association of American Railroads
AASHTO	American Association of State Highway and Transportation Officials
ACAMS	Automated Critical Asset Management System
AFSD-LE	Assistant Federal Security Directors for Law Enforcement
AFSP	Alien Flight Student Program
AGA	American Gas Association
AIP	Airport Improvement Program
AIS	Automated Identification System
AMSC	Area Maritime Security Committee
AMSP	Area Maritime Security Plan
ANSI	American National Standards Institute
AOPA	Airport Operators and Pilots Association
AOPL	Association of Oil Pipe Lines
APEC	Asia-Pacific Economic Cooperation
APGA	American Public Gas Association
API	American Petroleum Institute
APTA	American Public Transportation Association
ASAC	Aviation Security Advisory Committee
ASC	Airport Security Coordinator
ASI	Aviation Security Inspector
ASME	American Society of Mechanical Engineers
ASP	Airport Security Program
ASTM	American Society for Testing and Materials
ATS	Automated Targeting System
ATSA	Aviation and Transportation Security Act
ATU	Amalgamated Transit Union
AWW	America's Waterway Watch
BART	Bay Area Rapid Transit
BASE	Baseline Assessment and Security Enhancement
BIS	Bureau of Industry and Security
BZPP	Buffer Zone Protection Program

CARVER	Criticality, Accessibility, Recoverability, Vulnerability, Effect, and Reconcilability
CBP	Customs and Border Protection
CBRNE	Chemical, Biological, Radiological, Nuclear, and (High-Yield) Explosive
CCTV	Closed-Circuit Television
CD	Compact Disc
CDL	Commercial Driver's License
CFR	Code of Federal Regulations
CI/KR	Critical Infrastructure and Key Resources
CIP	Critical Infrastructure Protection
CIPAC	Critical Infrastructure Partnership Advisory Council
CISO	Chief Information Security Officer
CMC	Crisis Management Center
COBIT	Control Objectives for Information and Related Technology
COOP	Continuity of Operations
CR	Comprehensive Reviews
CSI	Container Security Initiative
CSR	Corporate Security Review
CTA	Chicago Transit Authority
CTAA	Community Transportation Association of America
C-TPAT	Customs-Trade Partnership Against Terrorism
DART	Dallas Rapid Area Transit
DCA	Ronald Reagan Washington National Airport
DEA	Drug Enforcement Administration
DHHS	Department of Health and Human Services
DHS	Department of Homeland Security
DNDO	Domestic Nuclear Detection Office
DOC	Department of Commerce
DoD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOS	Department of State
DOT	Department of Transportation

DPA	Defense Production Act
DSS	Decision Support System
EAT	Engineering Assessment Team
ECAC	European Civil Aviation Conference
EDS	Explosives Detection System
EMS	Emergency Medical Services
ESC	Executive Steering Committee
EU	European Union
FAA	Federal Aviation Administration
FACA	Federal Advisory Committee Act
FAF	Freight Analysis Framework
FAM	Federal Air Marshal
FAMS	Federal Air Marshal Service
FAS	Freight Assessment System
FBI	Federal Bureau of Investigation
FBO	Fixed-Base Operator
FDA	Food and Drug Administration
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
FHWA	Federal Highway Administration
FIG	Field Intelligence Group
FISMA	Federal Information Security Management Act
FIST	Field Intelligence Support Team
FLETC	Federal Law Enforcement Training Center
FMCSA	Federal Motor Carrier Safety Administration
FMSC	Federal Maritime Security Coordinator
FOUO	For Official Use Only
FPC	Federal Port Controller
FRA	Federal Railroad Administration
FRZ	Flight Restricted Zone
FSD	Federal Security Director
FSMP	Facility Security Management Program
FSR	Freight Security Requirement

FTA	Federal Transit Administration
FY	Fiscal Year
G8	Group of 8
G&T	Office of Grants and Training
GA	General Aviation
GA@DCA	Restoration of GA at Ronald Reagan Washington National Airport
GCC	Government Coordinating Council
GDP	Gross Domestic Product
GIS	Geographic Information Systems
GIWW	Gulf Intracoastal Waterway
GPRA	Government Performance Results Act
GPS	Global Positioning System
GTI	Gas Technology Institute
HACCP	Hazardous Analysis and Critical Control Point
HAZMAT	Hazardous Materials
HITRAC	Homeland Infrastructure Threat Risk Analysis Center
HOT	Hidden and Obviously Typical
HSAS	Homeland Security Advisory System
HSC	Homeland Security Council
HSIN	Homeland Security Information Network
HSPD	Homeland Security Presidential Directive
HTUA	High Threat Urban Area
I&A	Office of Intelligence and Analysis
IAC	Indirect Air Carrier
ICAO	International Civil Aviation Organization
ICC	Intelligence Coordination Center
ICE	Immigration and Customs Enforcement
ICS	Incident Command System
IED	Improvised Explosive Device
IFR	Instrument Flight Rules
IIIS-D	Integrated Intermodal Information System—Domestic
IMO	International Maritime Organization
INGAA	Interstate Natural Gas Association of America

IP	Office of Infrastructure Protection
IPMP	Integrated Protective Measures Plan
IPP	Infrastructure Protection Program
IPSLO	International Port Security Liaison Officer
ISAC	Information Sharing and Analysis Center
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
ISPS	International Ship and Port Facility Security
ISSO	Information System Security Officer
ISSP	Information Systems Security Program
IT	Information Technology
JPDO	Joint Planning and Development Office
JTTF	Joint Terrorism Task Force
JVA	Joint Vulnerability Assessment
LAN	Local Area Network
LES	Law Enforcement Sensitive
LLIS	Lessons Learned Information Sharing
LNG	Liquefied Natural Gas
LTATP	Land Transportation Anti-Terrorism Training Program
MANPAD	Man-Portable Air Defense System
MARAD	Maritime Administration
MARC	Maryland Rail Commuter
MARSEC	Maritime Security
MARTA	Metropolitan Atlanta Rapid Transit Authority
MAST	Maritime Analysis Support Tool
MBTA	Massachusetts Bay Transportation Authority
MDA	Maritime Domain Awareness
MIRP	Maritime Infrastructure Recovery Plan
MMCT	Multi-Modal Criticality Tool
MOU	Memorandum of Understanding
MSC	Maritime Security Committee
MSRAM	Maritime Security Risk Assessment Model
MSST	Maritime Safety and Security Team

MTS	Maritime Transportation System
MTSA	Maritime Transportation Security Act
MTSNAC	Marine Transportation System National Advisory Council
NADB	National Asset Database
NAS	National Airspace System
NCIP	National Critical Infrastructure Protection
NCSD	National Cyber Security Division
NCTC	National Counterterrorism Center
NEDCTP	National Explosives Detection Canine Team Program
NETL	National Energy Technology Laboratory
NextGen	Next Generation Air Transportation System
NGATS	Next Generation Air Transportation System
NICC	National Infrastructure Coordination Center
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NISAC	National Infrastructure Simulation and Analysis Center
NIST	National Institute of Standards and Technology
NMSAC	National Maritime Security Advisory Committee
NMTSP	National Maritime Transportation Security Plan
NOA	Notice of Arrival
NOAA	National Oceanic and Atmospheric Administration
NORAD	North American Aerospace Defense Command
NPIAS	National Plan of Integrated Airport Systems
NPRA	National Petrochemical and Refiners Association
NPRN	National Port Readiness Network
NRC	National Resource Center
NRP	National Response Plan
NSF	National Science Foundation
NSMS	National Strategy for Maritime Security
NSPD	National Security Presidential Directive
NSPI	National Strategy for Pandemic Influenza
NSSE	National Security Special Event
NSTS	National Strategy for Transportation Security

NTI	National Transit Institute
NTIA	National Telecommunications and Information Administration
NTS	National Transportation System
OCC	Operations Control Center
OI	Office of Intelligence
OMB	Office of Management and Budget
ONG	Oil and Natural Gas
ONI	Office of Naval Intelligence
OPT	Office of Operational Process and Technology
OSC	Operation Safe Commerce
OSTP	Office of Science and Technology Policy
PART	Performance Assessment and Rating Tool
PCII	Protected Critical Infrastructure Information
PHMSA	Pipeline and Hazardous Materials Safety Administration
PPBE	Planning, Programming, Budgeting, and Execution
PSGP	Port Security Grants Program
PSI	Principal Security Inspector
R&D	Research and Development
R&DWG	Research and Development Working Group
R&RWG	Response and Recovery Working Group
RAMCAP	Risk Analysis Methodology for Critical Asset Protection
RASM	Risk and Strategy Matrix
RDD	Radiological Dispersal Device
RDT&E	Research, Development, Test, and Evaluation
RFID	Radio Frequency Identification
RMD	Risk Management Division
RMSC	Regional Maritime Security Coalition
RMSP	Risk Management Strategic Planning
RPM	Radiation Portal Monitor
RSC	Rail Security Coordinator
RSP	Rail Security Pilot
S&T	Science and Technology Directorate
SAAP	Security Analysis and Action Program

SAFETEA-LU	Safe, Affordable, Flexible, Efficient Transportation Equity Act: A Legacy for Users
SAI	Security Action Item
SAV	Site Assistance Visit
SBRM	Systems-Based Risk Management
SBU	Sensitive But Unclassified
SCADA	Supervisory Control and Data Acquisition
SCC	Sector Coordinating Council
SCOTS	Special Committee on Transportation Security
SD	Security Directive
SIDA	Security Identification Display Area
SIPT	Security Integrated Product Team
SLFC	State and Local Fusion Center
SPM	Sector Partnership Model
SPP	Security and Prosperity Partnership of North America
SRO	Strategic Risk Objective
SSA	Sector-Specific Agency
SSD	Systems Support Division
SSI	Sensitive Security Information
SSOA	State Safety Oversight Agency
SSP	Sector-Specific Plan
SST	Smart and Secure Trade Lanes
ST-ISAC	Surface Transportation Information Sharing and Analysis Center
STSI	Surface Transportation Security Inspection
T4	Transit Terrorist Tools and Tactics
TAPA	Technology Asset Protection Association
TARR	Terrorist Awareness Recognition and Reaction
TCLDR	Transit, Commuter, and Long-Distance Rail
TFSSP	Twelve-Five Standard Security Program
TIH	Toxic Inhalation Hazard
TRAM	Transit Risk Assessment Module
TRANSCAER	Transportation Community Awareness and Emergency Response
TRB	Transportation Research Board

TSA	Transportation Security Administration
TSGP	Transportation Security Grant Program
TSNM	Transportation Sector Network Management
TSOC	Transportation Security Operations Center
TSSD	Transportation Security Situation Display
TVC	Threats, Vulnerabilities, and Consequences
TWIC	Transportation Worker Identification Credential
UASI	Urban Area Security Initiative
USACE	U.S. Army Corp of Engineers
US-CERT	United States Computer Emergency Readiness Team
USCG	U.S. Coast Guard
USDA	U.S. Department of Agriculture
USFORSCOM	U.S. Forces Command
USNORTHCOM	U.S. Northern Command
USTRANSCOM	U.S. Transportation Command
UTC	University Transportation Center
VBIED	Vehicle-Borne Improvised Explosive Device
VBST	Vessel Boarding and Security Team
VIPR	Visible Intermodal Prevention and Response
ViSAT	Vulnerability Identification Self-Assessment Tool
VTS	Vessel Traffic System
WAN	Wide Area Network
WCO	World Customs Organization
WMATA	Washington Metropolitan Area Transit Authority
WMD	Weapon of Mass Destruction

Appendix 2: Glossary of Key Terms

Some of the definitions in this glossary are derived from language enacted in Federal laws and/or included in national plans, including the Homeland Security Act of 2002, USA PATRIOT Act of 2001, the National Incident Management System, the National Response Plan, and the National Infrastructure Protection Plan.

Asset. An asset is any person, facility, material, information, or activity that has a positive value to the Transportation Systems Sector. The asset may have value to an adversary, as well as an owner, although the nature and magnitude of those values may differ. Assets may be categorized in many ways, including people, information, equipment, facilities, and activities or operations.

Consequence. The negative effect, or effects, that can be expected if an asset or system is damaged, destroyed, or disrupted.

Countermeasure. A countermeasure is an action intended to induce institutional, process, and physical changes that reduce risks to systems and assets. The countermeasure may address a vulnerability, threat, consequence, or overall system performance.

Critical Infrastructure. Assets, systems, and networks, whether physical or virtual, so vital to the United States that the incapacity or destruction of such assets, systems, or networks would have a debilitating impact on security, national economic security, public health or safety, or any combination of those matters.

Cyber Security. The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information contained therein to ensure confidentiality, integrity, and availability. Includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and September 11 communications and control systems.

Dependency. The one-directional reliance of an asset, system, network, or collection thereof, within or across sectors, on input, interaction, or other requirement from other sources in order to function properly.

Function. The service, process, capability, or operation performed by specific infrastructure assets, systems, or networks.

Government Coordinating Council (GCC). The council comprised of representatives across various levels of government (Federal, State, local, and tribal) as appropriate to the security and operational landscape of each individual sector. The GCC is the government counterpart to the Sector Coordinating Council (SCC) for each sector established to enable interagency coordination.

Impact. See consequence.

Interdependency. The multi- or bi-directional reliance of an asset, system, network, or collection thereof, within or across sectors, on input, interaction, or other requirement from other sources in order to function properly.

Key Resources. Publicly or privately controlled resources essential to the minimal operations of the economy and government.

Materiality. Materiality is a function of consequence and likelihood. Strategic risks have a very high materiality (i.e., very significant consequence and high likelihood), whereas traditional risks have low materiality (i.e., low consequence and/or low likelihood).

Mega-Node. The single point at which multiple modes intersect. In transportation systems, a mega-node is a place of potential failure or bottleneck, with the potential for wide-ranging disruptions and losses.

Mitigation. Activities designed to reduce or eliminate risks to persons or property or to lessen the actual or potential effects or consequences of an incident. Mitigation measures may be implemented prior to, during, or after an incident and are often developed in accordance with lessons learned from prior incidents. Mitigation involves ongoing actions to reduce exposure to, probability of, or potential loss from hazards. Examples of mitigation measures include zoning and building codes, floodplain buyouts, analysis of hazard-related data, and educating the public.

Mode. A specific form or variety of something. In the context of transportation, there are six modes: aviation, maritime, mass transit, highway, freight rail, and pipeline.

Network. A group of assets or systems that share information or interact with each other in order to provide infrastructure services within or across sectors.

Node. A network intersection or junction (e.g., a subway station).

Resilience. The capability of an asset, system, or network to maintain its function during or to recover from a terrorist attack, natural disaster, or other incident.

Risk. A measure of potential harm that encompasses threat, vulnerability, and consequence. In the context of the Transportation Systems Sector-Specific Plan (SSP), risk is the expected magnitude of loss due to a terrorist attack, natural disaster, or other incident, along with the likelihood of such an event occurring and causing that loss within or utilizing the sector.

Risk Management. The process of selecting and implementing security countermeasures to achieve an acceptable level of risk at an acceptable cost.

Risk Views. Risk views describe types of systems in terms of mode, geography, function, and ownership. These four views capture multiple ways of addressing systems and allow for a robust assessment of the Transportation Systems Sector.

Sector. The logical collection of assets, systems, or networks that provide a common function to the economy, government, or society. The Transportation Systems Sector is one of 17 critical infrastructure and key resources (CI/KR) sectors.

Sector Coordinating Council. The private sector counterpart to the GCC, this council is a self-organized, self-run, and self-governed representative of the sector's key stakeholders.

Sector Partnership Model. The framework used to promote and facilitate sector and cross-sector planning, coordination, collaboration, and information sharing for CI/KR protection involving all levels of government and private sector entities.

Sector-Specific Agency (SSA). Federal departments and agencies identified in Homeland Security Presidential Directive 7 (HSPD-7) as responsible for CI/KR protection activities in specified

CI/KR sectors. The sector-specific agency for transportation is the Transportation Security Administration (TSA).

Sector-Specific Plan (SSP). The augmenting plan that complements and extends the National Infrastructure Protection Plan (NIPP) Base Plan, detailing the application of the NIPP framework specific to each CI/KR sector. SSPs are developed by the SSAs in close collaboration with other security partners. This document is the SSP for the Transportation Systems Sector.

Security Partner. Federal, State, regional, Territorial, local, or tribal governmental entities; private sector owners and operators; and representative organizations, academic and professional entities, and certain not-for-profit private volunteer organizations that share in the responsibility for protecting the Nation's CI/KR.

Strategic Risk. Those risks that impact the entire Transportation Systems Sector, threatening disruption across multiple stakeholder communities. The consequences of strategic risks can cross multiple sectors and can have far-reaching, long-term effects on the national economy, natural environment, or public confidence. Strategic risks are those that breach the threshold of risks that stakeholders are reasonably expected to manage on their own and move into an area of risk management. Illustrative examples of strategic risks to the sector could include: disruption of a mega-node in the transportation system (large-scale impact on national economic security), use of a component of the transportation system as a weapon of mass destruction (terrorism event leading to loss of life and of public confidence), and release of a biological agent at a major rail transfer station or hub airport (terrorism event affecting national public health and safety).

Strategic Risk Objective (SRO). A measurable target that, when attained, contributes to the accomplishment of a strategic goal.

System. A collection of assets that comprises a dynamic, complex, and unified whole. A system maintains its existence and functions as a whole through the interaction of its parts.

Systems-Based Risk Management (SBRM). A risk management framework that helps define and clarify countermeasure programs aimed at a specific SRO, which will be integrated into the sector's strategic plan. SBRM is an important element of the sector's approach to determining its risk priorities, documenting them as SROs, determining approaches for achieving these objectives, and defining what success means for each of the SROs through performance measures. The SBRM process yields strategic countermeasures.

Threat. The intention and capability of an adversary to undertake actions that would be detrimental to CI/KR.

Transportation. Conveyance of passengers or goods. There are six modes of transportation: aviation, maritime, mass transit, highway, freight rail, and pipeline.

Transportation Security Incident. A security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area.

Vulnerability. A vulnerability is a characteristic or flaw that renders an asset or system susceptible to destruction, incapacitation, or exploitation.

Appendix 3: Transportation Systems Sector Assessment Tools and Methodologies

The Transportation Systems Sector and its partners in the homeland security community use a number of different tools and methodologies to assess threats, vulnerabilities, and consequences to assist the Nation's CI/KR owners and operators in assessing the risk to their infrastructures. The DHS is working closely with Federal, State, and local emergency responders; law enforcement; private sector associations; owners and operators; and other regional officials to use these tools, as well as to identify the requirements for developing new tools to assess the risks to critical transportation infrastructure.

The sector currently uses a number of tools to assess threats, vulnerabilities, and consequences, and calculate the risk to the transportation infrastructure. Stakeholders use many of these tools voluntarily, and the sector provides them to public and private owners and operators at no expense. Government assessors use some tools and methodologies specifically to enforce regulations or to provide free technical expertise and education in conducting a risk assessment effectively. Methodologies will continue to be appropriately vetted before the sanctioning of any transportation subsector. TSA will work with the DHS to find and leverage similarities between the different tool sets now in use as the sector organizes and adopts a system-wide risk assessment approach.

Although not all-inclusive, the following paragraphs briefly describe some of the analysis tools that TSA and its key Federal partners use to assess risk within the sector.

Analytical Risk Management

Tool:	*ARM*
Agency:	*Originally developed by the CIA Center for Security Excellence*
Type:	*Self-Assessment Tool*
Tool Assesses:	*Risk*

Analytical Risk Management methodology is based on the CIA Analytical Risk Management process. The process consists of six steps that result in the identification of risk associated with vulnerability and effective countermeasures that the leadership can apply to mitigate the risk. Each assessment requires a tailored approach for the specific sector being assessed. Every sector has differences—processes, information, facilities, raw materials, end products, operating principles, and procedures that make it unique. The analytical risk management process is specifically tailored to each of these differences. Throughout the process, each step and function is documented to provide an audit trail of the security decisions that are made.

CARVER Target Analysis and Vulnerability Assessment Tool

Tool:	*CARVER*
Agency:	*TSA, numerous other agencies and organizations*
Type:	*Self-Assessment and Government-Conducted Analytic Methodology*
Tool Assesses:	*Vulnerability and Consequence*

The Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability (CARVER) methodology is widely used throughout the Transportation Systems Sector as an easily employable methodology for owner/operators and Federal assessors to assess vulnerabilities and consequences against different threat scenarios. Often used by U.S. Special Operations Forces to target enemy installations or facilities or by force protection specialists to assess vulnerabilities from an adversary's point of view, TSA currently uses CARVER to assess the vulnerabilities and criticality of processes within the rail sector. As these factors are considered, they receive a numerical value related to the attractiveness of attacking the target. After all of the elements of a particular site are assessed against these factors, the site with the highest sum of values will be the most attractive target within the limits of that particular threat scenario.

Comprehensive Reviews

Tool:	*Comprehensive Review Process*
Agency:	*DHS; TSA and Transportation Stakeholders*
Type:	*Government-Facilitated Risk Assessment Tool*
Tool Assesses:	*Vulnerability, Consequence, and Risk (system level); Threat provided by TSA*

DHS Comprehensive Reviews contribute to the security of our Nation's critical infrastructure by thoroughly evaluating each significant facility's security; comparatively analyzing risk across the sectors; coordinating with Federal, State, and local response and recovery officials; identifying potential enhancements to security that can be made; and identifying additional measures that may protect against and mitigate the effects of terrorist attacks should they occur. The reviews enable the most effective allocation of homeland security resources. The Transportation Systems Sector began applying this tool in June 2006.

The Comprehensive Review process requires significant participation from private sector owners and operators, as well as Federal, State, and local officials. The GCCs of various sectors undergoing reviews work in close cooperation with their corresponding SCCs to foster participation in the review process. The Comprehensive Review team meets before the site visit and reviews the consequence and vulnerability information that the facility owner/operator provides, as well as the various pre-existing security and emergency response plans.

Each Comprehensive Review uses a standard set of tools and templates to develop a comparable estimate of the facility's vulnerability to a variety of threats, the range of consequences related to the threats, and an evaluation of existing security and response. The process provides a vehicle for discussion with stakeholders on potential enhancements to security in and around the site. This framework assists in reducing vulnerabilities, implementing appropriate security measures, and mitigating the potential consequences of a successful attack. To conduct a Comprehensive Review, a number of tools can be used, including the Vulnerability Identification Self-Assessment Tool (ViSAT) and eventually Risk Analysis and Management for Critical Asset Protection (RAMCAP).

After performing its site assessments, the Comprehensive Review team analyzes the information gathered and develops reports in both classified and For Official Use Only versions. The information is shared with appropriate stakeholders, including Federal agencies, State and local law enforcement, emergency management, and the facility owner/operators. Some outputs created from this process include:

- The site-specific Integrated Protective Measures Plan (IPMP) that identifies shortfalls in resources, evaluates response capabilities, and coordinates all agency-specific response plans**,** as well as training needs and options to address security and response challenges**;**
- The planning, tracking, and measurement of security and response enhancements in addition to the impact they have on the security and risk standing of the site**;** and

- Standardized risk data to enable a cross-sector comparative risk assessment, and investment and budgeting decisions.

Constellation/Automated Critical Asset Management System (ACAMS)

Tool:	*Constellation/ACAMS (pilot)*
Agency:	*DHS; State, Local, Tribal, Private Sector*
Type:	*Self-Assessment Tool and Training*
Tool Assesses:	*Vulnerability*

Through Operation Archangel, a pilot program and partnership between the DHS and the Los Angeles Police Department, assessors in the local police department and the National Guard are trained to conduct vulnerability assessments of critical State and local infrastructure to populate the ACAMS database. This pilot supports local and rural communities in identifying critical assets, assessing vulnerabilities, and developing preparedness programs at the local level. The focus is on collecting and communicating the necessary information required by an incident commander both pre-incident, in terms of protection plans and operational guides, and post-incident, as information required for effective response, mitigation, and recovery. Once these sites are assessed, the data can be supplied through ACAMS, providing improved domain awareness through an information portal. The ACAMS pilot is a secure online database that allows for storing, organizing, and using critical asset assessment information, and deploying that information to first-responders to improve preventive, security, and response activities.

Cross-Border Pipeline Infrastructure Vulnerability Assessments

Tool:	*Pipeline Assessment Tool*
Agency:	*DOE; TSA*
Type:	*Government Site Assessment*
Tool Assesses:	*Vulnerability*

The DOT and TSA are working with the DHS and DOE to gain domain awareness of the Nation's pipeline infrastructure system, identify vulnerabilities in U.S. and cross-border pipeline infrastructure, and review pipeline industry security plans and programs. TSA's Pipeline Security Division, along with pipeline security agencies from Canada, is participating in conferences and pipeline facility visits to assess the assets, threats, and vulnerabilities of the trans-border pipeline systems. TSA is the lead agency working with the DHS Office of Intelligence and Analysis (I&A) and the DOE Office of Energy Assurance (OEA), through the Smart Border Declaration's Energy Sector Working Group to deter terrorists from attacking the trans-border energy infrastructure through heightened domain awareness and improved security posture along national borders. Additionally, TSA coordinates tri-national pipeline vulnerability assessment visits with DOE/OEA, DHS/I&A, and Canadian and Mexican government agencies to evaluate cross-border pipeline operators' security plans and emergency response readiness.

Facility Security Management Program (FSMP)

Tool:	*Aviation Risk Assessment*
Agency:	*DHS; FAA; DOT*
Type:	*Government-Assisted Assessment Tool*
Tool Assesses:	*Risk*

Facilities are prioritized based on the impact that damage, loss of a facility, or disruption of the operation would have on air traffic. Included in the prioritization is how readily the asset or the function it performs can be replaced. The assessment of the facility's criticality (or priority) and other risk factors are then translated into facility security levels that drive the minimum required security measures for that facility. To determine the risk level of a particular facility, a systematic assessment of the threat and vulnerability is conducted. This evaluation includes a valid intelligence assessment of the general terrorist threat and an evaluation of any specific terrorist threat information available. Additionally, criminal threat evaluation is conducted by researching verified reportable incidents and criminal statistical data.

The overall results of the analysis are formulated into a risk rating for each facility. This risk rating is then used to determine what types of security measures are needed and whether additional security measures are required for a particular facility. A comprehensive program of scheduled and unscheduled on-site facility security assessments and inspections is conducted to ensure that the facility has implemented the required security measures based on its prioritization and threat assessment. If all required security measures have been fully implemented, then the facility is issued accreditation. If all required security measures have not been implemented, then a set of findings are developed and tracked until appropriate resources can be applied to implement the measures. Compliance is continually monitored through a comprehensive program of scheduled and unscheduled facility security assessments and inspections.

Federal Aviation Administration (FAA) Information Systems Security Program (ISSP)

Tool:	*Aviation Risk Assessment*
Agency:	*DHS; FAA; DOT*
Type:	*Government-Assisted Assessment Tool*
Tool Assesses:	*Risk*

The ISSP covers all air traffic control systems, including the operational, mission support, and business/administrative elements. There are six phases to the ISSP, and each phase is applied to implemented systems:

5. **Assessment**. During the assessment phase, information is gathered about a system and a risk assessment is performed. Then, recommendations are developed to mitigate or remediate identified risks.
6. **Security Planning**. During the security planning phase, the system architecture, information sensitivity, and management and operational controls needed to safeguard the system are determined.
7. **Remediation**. During the remediation phase, changes are made to the system based on the risk management/remediation recommendations. The system also undergoes testing to help identify any residual risks that may remain.
8. **Certification**. During the certification phase, the designated approving authority for the system determines whether the residual risks are acceptable and whether the system should be authorized for operational use.
9. **Deployment and Commissioning**. During deployment and commissioning, agreements are reached with other organizations for making specific changes to the system to enable it to connect and interoperate with other air traffic control systems and networks.
10. **Post-Authorization**. The last phase, the post-authorization phase, is to ensure that the system continues to operate as intended and that no new risks have arisen or been introduced.

Federal Highway Administration (FHWA) Bridge and Tunnel First-Responder Workshops

Tool:	*First-Responder Awareness to Terrorist Threats for Bridges and Tunnels Workshop*
Agency:	*DOT; FHWA*
Type:	*Government Instruction on the Identification of Threats and Vulnerabilities to Bridges and Tunnels and Mitigation Approaches*
Tool Assesses:	*First-Responder Threat Awareness*

The ½-day-long workshop is designed to give first-responders, such as law enforcement personnel, inspectors, and other emergency responders, an overall awareness of terrorist threats and structural vulnerabilities. More specifically, they will learn to identify the strengths and weaknesses of bridge and tunnel components, estimate the damage to be expected for terrorist threats, and analyze the risk of each component to a specific threat. Threats covered include the vehicle-borne improvised explosive devices (IEDs), hand-placed IEDs, non-explosive cutting devices, fire, and vehicle impact.

Federal Highway Administration (FHWA) Bridge and Tunnel Vulnerability Workshops

Tool:	*FHWA Risk Management for Terrorist Threats to Bridges and Tunnels Workshops*
Agency:	*DOT; FHWA*
Type:	*Government Instruction on Assessment Tool Usage*
Tool Assesses:	*Vulnerability and Risk by Design*

The Risk Management for Terrorist Threats to Bridges and Tunnels Workshop is 1½ days long and is designed to give engineers and managers the understanding to develop a cost-effective risk management plan for a structure using component-level analysis. More specifically, they will learn to identify strengths and weaknesses of bridge and tunnel components estimate the damage to be expected for terrorist threats, and analyze the risk of each component with regard to a specific threat. Threats covered include vehicle-borne IEDs, hand-placed IEDs, non-explosive cutting devices, fire, and vehicle impact.

Federal Highway Administration (FHWA) Statewide and Project-Specific Vulnerability Assessments

Tool:	*Highway, Bridge, and Tunnel Vulnerability Assessments*
Agency:	*DOT; FHWA*
Type:	*Government-Assisted Site Visit Assessment*
Tool Assesses:	*Vulnerability*

An FHWA-trained cadre of engineers stands ready to assess bridges and tunnels for vulnerability to terrorist threats. DOT engineers, at the request of State transportation leaders, assess the vulnerabilities of highway assets (signature bridges, tunnels, and key intermodal freight transfer facilities; traffic control systems) and prioritize security needs. This Engineering Assessment Team (EAT) performs assessments, at the request of the owners, for project-level, facility-level, and statewide critical structures. To date, the aim has been to guide the owners and operators to identify vulnerable components and recommend measures to reduce those vulnerabilities. The team also provides technical support to the USCG for its port security assessments.

Freight Analysis Framework (FAF)

Tool:	*FAF Version 1*
Agency:	*DOT; FHWA*
Type:	*Government-Conducted Analysis Tool*
Tool Assesses:	*Consequence*

FAF acts as a surface transportation consequence analysis tool to estimate commodity flows and related transportation activities among State, sub-State regions, and major international gateways on the Nation's transportation infrastructure facilities. FAF identifies how commodities are moved from origin to destination through the highway network. It can also be used to conduct scenario analysis with regard to disabling any roadway links (highway segment, bridges) and nodes (interchanges and intersections) covered by the FAF highway network. This scenario analysis produces a number of key insights, including identifying critical nodes in the surface transportation arena, possible alternative routes, the number of affected trucks, congestion both upstream and downstream of the affected links/nodes, tonnage and dollar value of the commodities affected, types of commodities being affected, additional travel time, and a new congestion outlook throughout the network. The highway network where these commodities are transported includes all interstate highways and all principal arterials. The network covers more than 450,000 miles of roadway.

The FAF commodity data are measured in terms of annual average daily movement. Any analysis based on such data is an assessment for a typical average day. It takes substantial effort to organize both the network and commodity origin destination data to run an FAF scenario analysis. For a single scenario analysis, it is expected to take a minimum of a full workday. Currently, FHWA is updating the original FAF (FAF1) to provide more accurate and complete pictures of freight movement in the Nation. While FAF2 is under development, FAF1 is still operational.

Hazard Analysis and Critical Control Points (HACCP) Methodology

Tool:	*HACCP (for freight rail; piloting for long-distance passenger rail)*
Agency:	*TSA*
Type:	*Government-Conducted Analytic Methodology*
Tool Assesses:	*Risk*

TSA uses a system-oriented risk HACCP methodology to determine the security risks associated with movement of maritime containers and toxic inhalation hazard (TIH) chemicals by rail. HACCP, and its accompanying metrics, was a collaborative development effort drawing on expertise from the DHS and DOT, with the input of numerous railroad career specialists and subject matter experts with perspectives ranging from railway industry management, security, and regulatory oversight. This methodology provides a process for determining which points in a particular freight rail system are the most critical to protect and offers a general view of security options to control the catastrophic breach of a TIH railcar exposing hazardous cargo to the atmosphere. The analysis focuses on using explosives to cause the TIH breach; however, other means are also assessed. The analysis also captures the potential consequences and plume size of the release. The methodology accounts for physical security measures, the critical node's infrastructure characteristics, impact on rail operations, symbolic importance, proximity to other CI/KR, and other variables. Surface Transportation Security Inspectors are also adapting a version of HACCP that FTA uses for application with long-distance passenger rail, as well as a more involved impact analysis for implementing different types of countermeasures.

Hazardous Materials Transportation Risk Management Self-Evaluation Framework

Tool:	*Risk Management Self-Evaluation Framework (RMSEF) Security Template*
Agency:	*DOT; Pipeline and Hazardous Materials Safety Administration (PHMSA)*
Tool Assesses:	*Vulnerabilities and Strategies to Mitigate Risks*

PHMSA's Hazardous Materials Regulations (HMRs) require shippers and carriers of certain hazardous materials to develop and implement security plans that consider risks related to transportation of hazardous materials in commerce. The security plan must address personnel security, en route security, and unauthorized access. Shippers and carriers subject to the security plan requirement must perform an assessment of the transportation security risk associated with the materials they handle. The RMSEF Security Template provides principles and structure illustrating how a risk management methodology can be used to identify points in the transportation process where security procedures should be enhanced within the context of an overall risk management strategy.

IDEF0

Tool:	*IDEF0 (Integration Definition for Functional Modeling)*
Agency:	*Department of Commerce, FIPS 183*
Type:	*Self Assessment*
Tool Assesses:	*Organizational Processes and Functions*

IDEF0 (Integration Definition Language 0) is based on the Structured Analysis and Design Technique (SADT) and includes both a definition of a graphic modeling language and a description of a comprehensive methodology for developing models for a wide variety of automated and non-automated systems. It is comprehensive and expressive, capable of representing a wide variety of business, manufacturing, and other types of enterprise operations to any level of detail. IDEF0 provides a means for completely and consistently modeling the functions required by a system or subject area and the data and objects that interrelate with those functions.

Joint Vulnerability Analysis (JVA)

Tool:	*Joint Vulnerability Analysis*
Agency:	*TSA (with FBI assistance as needed)*
Type:	*Government-Conducted Field Assessment*
Tool Assesses:	*Vulnerability*

JVA will be applied at all commercial airports, focusing initially on the nationally critical airports. As required by legislation, JVA is applied jointly by TSA Aviation Operations personnel and FBI personnel. JVA uses current, FBI-developed threat information as its starting point and then focuses on defining an airport's security system in detail. Once the airport's security system is defined, JVA examines the security system against a current threat required to complete the given threat. Using a ViSAT-shell for the assessment, once the airport's security system is defined, JVA focuses on examining security system against current threats.

Maritime Security Risk Assessment Model (MSRAM)

Tool:	*MSRAM*
Agency:	*USCG*
Type:	*Government-Applied Risk Assessment Tool*
Tool Assesses:	*Threat, Vulnerability, Consequence, and Risk*

MSRAM is a risk analysis tool used to analyze strategic, operational, and tactical risks within and across U.S. ports that allows risk managers and decisionmakers to understand the geographic density of risk across the Nation's ports, the profile of risk within a port, and asset-specific risk to help identify maritime CI/KR. The tool is designed to allow a port-level user to assess risk based on the threat, vulnerability, and consequence factors associated with a target (asset) in the maritime domain. The assessor uses scenarios, pairing an asset and attack mode in combination. Each scenario is analyzed to determine threat, vulnerability, consequence, area-wide security, and response capabilities.

Threat is computed using data from the USCG Intelligence Coordination Center using terrorist intent and capability. Consequence is computed by analyzing the primary consequence and the secondary economic impact of an attack. In the analysis, the following factors are considered: death and injury, primary economic impact, symbolic effect, national security, environmental impact, response capabilities, recoverability, redundancy, and secondary economic impact. Vulnerability is computed by analyzing the achievability of the attack, system security, and target hardness. Local risk data are collected in such a way that it can be used to inform both local and national risk analysis needs and feed the risk management process within the maritime domain.

Multi-Modal Criticality Tool (MMCT)

Tool:	*MMCT*
Agency:	*TSA*
Type:	*Government-Conducted Assessment Tool*
Tool Assesses:	*Consequence*

TSA's strategic risk assessment approach begins by assessing *consequences* to identify assets that are most important to protect from attack. Starting with the former FBI National Infrastructure Protection Center (NIPC) tool, TSA worked with the DHS/IP to develop MMCT in 2003. MMCT provides an assessment of a target's potential importance and the consequences of a worst case, plausible threat. The rating scheme considers aspects from five categories of consequence (e.g., loss of life, economic impact). Criticality determinations are not solely numbers driven; human experience is taken into consideration using a subject matter expert review panel before headquarters analysts make a final determination. Over the last 2 years, TSA has completed more than 2,500 criticality assessments, including one on the Nation's major commercial airports. Applying MMCT to transportation assets was an integral element in determining the Top 100 list of the Nation's critical transportation infrastructures, an effort completed in full collaboration with DOT, USCG, and USTRANSCOM.

Risk Analysis and Management for Critical Asset Protection (RAMCAP)

Tool:	*RAMCAP Module for Transportation*
Agency:	*DHS*
Type:	*Government-Facilitated Risk Assessment Tool*
Tool Assesses:	*Vulnerability, Consequence, and Risk; Threat provided by the DHS/HITRAC*

The DHS is currently developing RAMCAP, a risk framework that the owners and operators of the Nation's critical infrastructure can use to assess terrorist risk to their own assets and systems. This will allow the DHS to normalize and prioritize assets across all 17 critical infrastructure sectors. This process allows owners and operators—who are most cognizant of asset composition and security—to provide the bulk of the information for consequence and vulnerability, given that the DHS provides any of the attack scenarios. The DHS, in turn, will provide an estimate of threat likelihood, representing the judgment of the intelligence community for relative possibility of various attacks against assets of certain types, which will figure critically in owner/operator and DHS evaluations of risk associated with a particular asset. RAMCAP development currently resides with the American Society of Mechanical Engineers (ASME). The DHS is currently using RAMCAP in the Nuclear Reactors, Materials, and Waste Sector and piloting the tool in the Chemical Sector. To date, no RAMCAP transportation modules have been developed, but their development is being planned.

RAMCAP can be considered an asset-driven approach to evaluating risk, since the intrinsic qualities of an asset, rather than the likelihood of a threat, govern the evaluation. Consequence and vulnerability estimates will remain relatively static; variables relative to threat likelihood can be periodically updated to account for the risk-reduction impact of security measures. RAMCAP results allow the DHS and other Federal agencies to prioritize assets from different sectors based on comparative risk analyses. This will, in turn, allow the DHS and other agencies to implement security measures and employ our Nation's resources in a manner that maximizes the allocation of limited resources for the security of the Nation.

Site Assistance Visits (SAVs)

Tool:	*SAV*
Agency:	*DHS (RMD)*
Type:	*Government-Conducted Assessment*
Tool Assesses:	*Vulnerability*

The SAV is an inside-the-fence vulnerability assessment that addresses both the static and dynamic vulnerabilities of a particular site. The SAV is also designed to facilitate vulnerability identification and mitigation discussions between government and industry in the field. It is a qualitative and easy-to-use process that leverages proven techniques; expert knowledge; facility-specific data; hands-on exercises; and all available information, including previously conducted vulnerability assessments. Fifty-three SAVs have been completed in the sector, including aviation, passenger rail, freight rail, and highway bridges and tunnels.

Transit Risk Assessment Module (TRAM) Tool Kit

Tool:	*TRAM (MAST for maritime application)*
Agency:	*DHS G&T; State and Local Authorities*
Type:	*Self-Assessment Tool*
Tool Assesses:	*Risk*

The DHS developed TRAM (and the Maritime Analysis Support Tool (MAST)) to provide a comparative assessment of risk between critical mass transit assets to assist owners and operators in the challenge of prioritizing scarce resources. The DHS developed the tool kit using a best practices approach of risk assessment methods from throughout the Federal Government. This self-assessment tool provides methods for owner/operators to conduct consequence, threat, vulnerability, response and recovery, and impact assessments. Finally, these results can inform a risk assessment, allowing the assessor to prioritize needs and resources. While the tool measures risk on a relative basis, such as the likelihood of one attack type occurring versus another, this tool does not make direct dollar-to-dollar cost-benefit comparisons.

Transportation Security Administration (TSA) Corporate Security Reviews (CSRs)

Tool:	*CSR*
Agency:	*TSA*
Type:	*Government-Assisted Self-Assessment Tool*
Tool Assesses:	*Vulnerability, Consequence, and Risk (when Threat is provided by TSA)*

The CSR process assists TSA risk assessors in identifying risks, preparing mitigation strategies, and prioritizing security needs. The CSR process is used with the goal of hosting face-to-face meetings with key stakeholders to review their security plans. This process helps TSA and the DHS to better identify the assets at greatest risk across the country and improve their security capabilities. CSR objectives include efforts to validate implementation of corporate security plans, gather data for intra/intermodal trend analysis, identify security gaps and offer mitigation options, and promote domain awareness and outreach to sector stakeholders. TSA's CSR program has reviewed more than 60 percent of State departments of transportation, and has been expanded to pipelines and motor carriers of freight and passengers, including schoolbus operations. CSR visits serve to collect physical and operational preparedness information, critical assets, and key point-of-contact lists; review emergency procedures; conduct domain awareness training; and provide an opportunity to share industry best practices. TSA's program is instructive for all entities engaged in transportation by motor vehicle or those that maintain or operate key physical assets within the highway transportation and pipeline community. The CSR is a voluntary event and is conducted at the invitation of the owner or operator of the physical structure or operating entity. CSR files serve as the only universal baseline security data repository available within the partnership of Federal agencies and they assist in developing security standards and measuring compliance.

Vulnerability Identification Self-Assessment Tool (ViSAT)

Tool:	*ViSAT*
Agency:	*TSA*
Type:	*Self-Assessment Risk Assessment Tool*
Tool Assesses:	*Vulnerability, Consequence, and Risk (Threat provided by TSA)*

ViSAT is a voluntary Web-based, self-assessment tool that guides a user through a series of security-related questions to develop a comprehensive security baseline evaluation of a transportation entity's current level of security. ViSAT focuses on the prevention and mitigation of a base array of threat scenarios developed for various subcategories of transportation modes, known as ViSAT modules.

These owner/operator-conducted self-assessment risk modules enable users to assess their baseline security system's effectiveness in direct response to specific threat scenarios. Users are required to rate their asset in terms of target attractiveness (from a terrorist's perspective) and several consequence categories that broadly describe health and well-being, economic consequence, and the symbolic value of the vessel or facility. The security system's effectiveness is then reassessed based on the asset's baseline security countermeasures for each threat scenario and then rated on the effectiveness of each countermeasure in detecting and preventing the terrorist's actions under heightened threat conditions corresponding to the Homeland Security Advisory System (HSAS).

The assessment is Web-based, allowing for easy uploading of information to TSA for more indepth analysis by TSA personnel, if desired. Once an assessment has been submitted to the DHS and approved, the information from that assessment will be linked to individual assets, and the system will allow the owner/operator to replicate like assets. The DHS has already deployed ViSAT for targeted maritime vessel and facility categories. The DHS intends to develop ViSAT modules for each of the remaining four transportation modes as well: Aviation, Highway, Freight Rail, and Pipeline. The ViSAT modules for mass transit (heavy rail); passenger rail; and highway bridges, operations centers, and rail passenger terminals are currently available.

Countermeasures deployed during a target-specific alert may have a detrimental effect on the asset's operations. The intention of the defined enhanced countermeasure set is to increase security effectiveness compared to the baseline security effectiveness ratings. Additional or enhanced countermeasures can be included in the security plan, along with estimated resource requirements and a timeframe for implementation. All assessments that are submitted will be verified for accuracy and consistency when compared against like assets. This verification process helps ensure that the data captured are accurate, and it assists users in avoiding potential pitfalls in their process.

Appendix 4: Additional Federal Security Partners

- **Defense Joint Intelligence Operations Center (DJIOC)**. DJIOC was established to integrate and synchronize military and national intelligence capabilities. DJIOC will plan, prepare, integrate, direct, synchronize, and manage continuous, full-spectrum Defense Intelligence Operations in support of the Combatant Commands (COCOM). This will be a collaborative, interactive relationship with the Office of the Director of National Intelligence (ODNI), national intelligence agencies and centers, Combatant Command JIOCs, Combat Support Agencies, the Armed Services intelligence organizations, and the Joint Functional Component Command for Intelligence, Surveillance, and Reconnaissance (JFCC-ISR) to create a system-of-systems JIOC enterprise network-enabled by enterprise information technology architecture.
- **Department of Agriculture (USDA)**. USDA sets public policy to protect the Nation's food supply, agricultural base, and natural resources. On January 30, 2004, HSPD-9 established a national policy to defend the agriculture and food system against terrorist attacks, disasters, and other emergencies. The directive also fosters a cooperative working relationship among the DHS, USDA, and the Department of Health and Human Services in expanding and conducting vulnerability assessments, mitigation strategies, and response planning. Since there are key interdependencies between the Transportation Systems Sector and the Food and Agriculture Sector and its component agencies (USDA, FDA), future planning efforts must consider integrating security policies and initiatives where appropriate between the two sectors.
- **Department of Commerce (DOC)**. DOC's National Institute of Standards and Technology (NIST) is conducting more than 75 projects that support law enforcement, military operations, emergency services, airport and building security, and cyber security. DOC's National Telecommunications and Information Administration (NTIA), through its research and engineering laboratory, is developing better communication systems for first-responders, improving public safety networks, and researching new uses of the Internet for public safety communications.
- **Department of Justice (DOJ)**. DOJ investigates and prosecutes criminal offenses and represents the Federal Government in litigation. The major investigative agencies—the FBI, the Drug Enforcement Administration (DEA), and the Bureau of Alcohol, Tobacco, Firearms, and Explosives—prevent and deter crime and apprehend criminal suspects. DOJ will contribute to the Transportation Systems Sector through its law enforcement role. In the national effort to identify, prevent, and prosecute terrorists within the Transportation Systems Sector, TSA will work closely with the FBI, who maintains lead responsibility for investigations of terrorists' acts or threats by individuals or groups inside the United States where such acts are within the Federal criminal jurisdiction of the United States.
- **Department of State (DOS)**. DOS conducts diplomacy—a mission based on the role of the Secretary of State as the President's principal foreign policy advisor. DOS leads representation of the United States overseas and advocates U.S. policies with foreign governments and international organizations. DOS plays an important role in coordinating transportation security issues with foreign governments and addressing issues concerning the security of pipelines that cross national boundaries.
- **Federal Law Enforcement Training Center (FLETC)**. FLETC provides basic and advanced training for Federal law enforcement agency personnel at the DHS and DOT. FLETC also provides training for State and local law enforcement officers and other security personnel.

Food and Drug Administration (FDA). FDA is responsible for carrying out certain provisions of the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (PL107-188), specifically Subtitle A (Protection of Food Supply) and Subtitle B (Protection of Drug Supply) of Title III. On January 30, 2004, HSPD-9 was released, establishing a national policy to defend the agriculture and food system against terrorist attacks, disasters, and other emergencies. TSA has participated in a number of meetings and focus/working groups with USDA and FDA to increase cooperation on security efforts for food/agricultural product transportation. Since there are key interdependencies between the Transportation Systems Sector and the Food and Agriculture Sector and its component agencies (USDA, FDA), future planning efforts must consider integrating security policies and initiatives where appropriate between the two sectors.

- **Homeland Infrastructure Threat and Risk Analysis Center**. HITRAC is the DHS's infrastructure-intelligence fusion center that maintains situational awareness of infrastructure sectors and develops long-term strategic assessments of their risks by integrating threat information with the unique vulnerabilities and consequences of attack for each infrastructure sector.
- **Immigration and Customs Enforcement (ICE)**. ICE is the DHS's largest investigative bureau. ICE includes the investigative and intelligence resources of the former U.S. Customs Service, the former Immigration and Naturalization Service, and the Federal Protective Service, bringing together more than 20,000 employees who focus on enforcing immigration and customs laws within the United States and the protection of specified Federal buildings.
- **National Counterproliferation Center (NCPC)**. NCPC coordinates strategic planning within the intelligence community to enhance intelligence support of U.S. efforts to stem the proliferation of weapons of mass destruction and related delivery systems. NCPC works with the intelligence community to identify critical intelligence gaps or shortfalls in collection, analysis, or exploitation, and to develop solutions to ameliorate or close these gaps. It also works with the intelligence community to identify long-term proliferation threats and requirements, and to develop strategies to ensure that the intelligence community is positioned to address these threats and issues. NCPC reaches out to elements both inside and outside of the intelligence community, and the government to identify new methods or technologies that can enhance the capabilities of the intelligence community to detect and defeat future proliferation threats.
- **National Counterterrorism Center (NCTC)**. NCTC serves as the primary organization in the Federal Government for integrating and analyzing all intelligence pertaining to terrorism and counterterrorism, and conducting strategic operational planning by integrating all instruments of national power.
- **National Geospatial-Intelligence Agency (NGA)**. NGA provides timely, relevant, and accurate geospatial intelligence (GEOINT) to support national security domestically and abroad. NGA's geospatial-intelligence products serve a variety of military, civil, and international needs. In terms of transportation security, GEOINT provides the fundamental properties of geographical location associated with the data critical to maintaining appropriate posture and awareness, and also provides the value-added analyses required to create a distinct type of actionable intelligence for time-sensitive transportation issues.
- **North American Aerospace Defense Command (NORAD)**. NORAD provides detection, validation, and warning of attacks against North America by aircraft, missiles, or space vehicles, and aerospace control of air-breathing threats to North America. NORAD obtains, processes,

assesses, and disseminates appropriate intelligence/information to provide timely warning of maritime threats or attacks against North America.

- **Office of Intelligence and Analysis**. The DHS's Office of Intelligence and Analysis ensures that information is gathered from all relevant field operations and other parts of the intelligence community; analyzed with a mission-oriented focus; is informative to senior decisionmakers; and is disseminated to the appropriate Federal, State, local, and private sector partners.
- **Office of Naval Intelligence (ONI)**. ONI supports joint operational commanders with a worldwide organization and an integrated workforce of active duty, reserve, officer and enlisted, and civilian professionals. At the National Maritime Intelligence Center (NMIC), ONI brings military and civilian employees into a single command to provide "one-stop shopping" for national-level maritime intelligence.
- **Science and Technology Directorate (S&T)**. S&T is the primary R&D arm of the DHS. It provides Federal, State, and local officials with the technology and capabilities to protect the homeland.
- **Surface Transportation Board (STB)**. When STB determines that a shortage of equipment, traffic congestion, unauthorized cessation of operations, or other failures of traffic management exist that creates an emergency situation of such magnitude as to have substantial adverse effects on shippers or on rail service in a region of the United States, or that a rail carrier cannot transport the traffic offered to it in a manner that properly serves the public, STB may, for up to 270 days, direct the handling, routing, and movement of the traffic of a rail carrier and its distribution over its own or other railroad lines, and give directions for preference or priority in the transportation of traffic.
- **U.S. Army Corps of Engineers (USACE)**. USACE is responsible for maintaining the Nation's commercial waterways, including levees, and operating the dams and locks that facilitate commerce on inland waterways.
- **U.S. Northern Command (USNORTHCOM)**. USNORTHCOM conducts operations to deter, prevent, and defeat threats and aggression aimed at the United States and its Territories and interests within the assigned area of responsibility; as directed by the President or Secretary of Defense, it provides military assistance to civil authorities, including consequence management operations. USNORTHCOM's area of responsibility includes air, land, and sea approaches and encompasses the continental United States, Alaska, Canada, Mexico, and the surrounding water out to approximately 500 nautical miles. It also includes the Gulf of Mexico and the Straits of Florida.
- **U.S. Pacific Command (USPACOM)**. USPACOM conducts operations to deter, prevent, and defeat threats and aggression aimed at the United States and its Territories and interests within the assigned area of responsibility. As directed by the President or Secretary of Defense, it provides military assistance to civil authorities, including consequence management operations. USPACOM's area of responsibility encompasses Hawaii and U.S. Territories, possessions, and freely associated states in the Pacific.
- **U.S. Transportation Command (USTRANSCOM)**. USTRANSCOM provides air, land, and sea transportation for the Department of Defense, both in times of peace and times of war, in support of the President and Secretary of Defense, and Combatant Commander-assigned missions.

Appendix 5: National Asset Database Transportation Taxonomy Quick Reference

11. TRANSPORTATION

11.1 AVIATION

11.1.1 Aviation Conveyances

11.1.2 Airports

11.1.2.1 Certificated Airports

11.1.2.1.1 Class I Airports

11.1.2.1.2 Class II Airports

11.1.2.1.3 Class III Airports

11.1.2.1.4 Class IV Airports

11.1.2.2 Non-Certificated Airports

11.1.2.2.1 Public Airports

11.1.2.2.2 Private Airports

11.1.2.3 Military Airfields

11.1.2.3.1 Air Force Airfields

11.1.2.3.2 Army Airfields

11.1.2.3.3 Navy Airfields

11.1.2.3.4 Marine Corps Airfields

11.1.2.3.5 Coast Guard Airfields

11.1.2.4 Foreign Airports

11.1.3 Air Traffic Control and Navigation Facilities

11.1.3.1 Air Route Traffic Control Facilities

11.1.3.2 Airport Traffic Control Towers

11.1.3.3 Flight Service Stations

11.1.3.4 Other Air Traffic Control Facilities

11.1.4 Space Transportation Facilities

11.1.4.1 Military Facilities

11.1.4.1.1 Launch Vehicles

11.1.4.2 Commercial Facilities

11.1.4.2.1 Launch Vehicles

11.1.5 Aviation Sector Command Control Communication Coordination Facilities

11.1.6 Other Aviation Facilities

11.2 RAILROAD

11.2.1 Railroad Conveyance

11.2.1.1 Freight Conveyance

11.2.1.2 Passenger Conveyance

11.2.1.2.1 Passenger Trains Long Distance/Intercity

11.2.1.2.2 Passenger Trains Commuter

11.2.2 Railroad Rights of Way

11.2.2.1 Railroad Track

11.3.2.2.1 Truck Terminal HAZMAT

11.2.2.1.1 STRACNET Track

11.2.2.1.2 Other Track

11.2.2.2 Railroad Bridges

11.2.2.3 Railroad Tunnels

11.2.3 Railroad Yards

11.2.3.1 Rail Yard – Local

11.2.3.2 Rail Yard – Classification

11.2.3.3 Rail Yard – Intermodal

11.2.3.4 Rail Yard – HAZMAT

11.2.4 Railroad Stations

11.2.4.1 Railroad Passenger Stations

11.2.5 Railroad Operations Centers

11.2.5.1 Railroad Dispatch and Operations Control Centers

11.2.5.2 Railroad Communications Centers

11.2.5.3 Railroad Signaling Facilities and Equipment

11.2.6 Other Railroad Facilities

11.3 ROAD

11.3.1 Roadways and Supporting Facilities

11.3.1.1 Roadways

11.3.1.1.1 Limited Access Highways

11.3.1.1.2 Multi-Lane Non-Limited Access Highways

11.3.1.1.3 Two-Lane Numbered Highways

11.3.1.1.4 Other Roads

11.3.1.2 Road Bridges

11.3.1.3 Road Tunnels

11.3.1.4 Highway Rest and Service Areas

11.3.1.4.1 Highway Rest Stops

11.3.1.4.2 Highway Service Areas

11.3.1.4.3 Vehicle Weigh Stations

11.3.1.5 Road Transportation Support Facilities

11.3.1.5.1 Operations and Traffic Management Centers

11.3.1.5.2 Road International Border Facilities

11.3.1.5.3 Motor Vehicle Fueling Stations

11.3.2 Trucking

11.3.2.1 Truck Conveyance

11.3.2.2 Truck Terminals Facilities

11.3.2.2.2 Truck Terminal Non-HAZMAT Facilities

11.3.2.3 Truck Rental Facilities
11.3.2.4 Truck Dispatch Centers
11.3.2.5 Truck Operations Centers
11.3.3 Over-the-Road Motorcoach System
11.3.3.1 Motorcoach Conveyance
11.3.3.2 Over-the-Road Motorcoach Passenger Terminals
11.3.3.3 Over-the-Road Motorcoach Facilities
11.3.3.3.1 Storage Facilities
11.3.3.3.2 Maintenance Facilities
11.3.3.4 Over-the-Road Motorcoach Operations Centers
11.3.3.5 Over-the-Road Motorcoach Dispatch Centers
11.3.4 School Bus Systems
11.3.4.1 School Bus Conveyance
11.3.4.2 School Bus Routes
11.3.4.3 School Bus Stops
11.3.4.4 School Bus Maintenance Facilities
11.3.4.5 School Bus Dispatch Centers
11.3.4.6 School Bus Communications Centers
11.3.5 Other Road Facilities
11.4 MARITIME
11.4.1 Vessels
11.4.1.1 Shallow Draft Vessels
11.4.1.1.1 Tugs and Towboats
11.4.1.1.2 Small Vehicle/Passenger Ferries
11.4.1.1.3 River Ferries
11.4.1.1.4 Excursion/Tour Boat
11.4.1.1.5 Supply/Work Boat
11.4.1.1.6 Recreational Vessel
11.4.1.1.7 Barge – Tank
11.4.1.1.8 Barge – Hopper
11.4.1.1.9 Barge – Gas
11.4.1.2 Deep Draft Vessels
11.4.1.2.1 General Cargo Ship
11.4.1.2.2 Container Ship
11.4.1.2.3 Dry Bulk Cargo Ship
11.4.1.2.4 Tank Ship
11.4.1.2.5 Gas Carrier Ship
11.4.1.2.6 Roll-On/Roll-Off and Pure Car Carrier
11.4.1.2.7 Cruise Ship
11.4.1.2.8 Large Vehicle/Passenger Ferries
11.4.1.2.9 Medium Vehicle/Passenger Ferries
11.4.1.2.10 Military Combatant Vessel
11.4.1.2.11 Military Support Vessels
11.4.1.2.12 Other Vessels
11.4.2 Ports
11.4.2.1 Shallow Draft Ports
11.4.2.1.1 Shallow Draft General Cargo Terminal
11.4.2.1.2 Shallow Draft Dry Bulk Cargo Terminal
11.4.2.1.3 Shallow Draft Liquid Bulk Cargo Terminal
11.4.2.1.4 Shallow Draft Barge Fleeting Area
11.4.2.1.5 Shallow Draft Passenger Terminal
11.4.2.2 Deep Draft Ports
11.4.2.2.1 Deep Draft General Cargo Terminal
11.4.2.2.2 Deep Draft Containerized Cargo Terminal
11.4.2.2.3 Deep Draft Dry Bulk Cargo Terminal
11.4.2.2.4 Deep Draft Liquid Bulk Cargo Terminal – Crude/Product
11.4.2.2.5 Deep Draft Liquid Bulk Cargo Terminal – Chemical
11.4.2.2.6 Deep Draft Bulk Gas Cargo Terminal
11.4.2.2.7 Deep Draft Industrial Cargo Terminal
11.4.2.2.8 Off-Shore Terminals or Platforms
11.4.2.2.9 Outer Continental Shelf Crude Oil Platforms
11.4.2.2.10 Outer Continental Shelf Natural Gas Platforms
11.4.2.2.11 Cruise Ship Passenger Terminal
11.4.2.2.12 Ferry Terminals
11.4.2.2.13 Military Cargo Terminal
11.4.2.2.14 Military Combatant Vessel Terminal
11.4.2.3 Port Public Access Areas
11.4.3 Waterways
11.4.3.1 Inland Waterways
11.4.3.2 Intracoastal Waterways
11.4.3.3 Canals
11.4.3.4 Locks
11.4.3.5 Dams
11.4.4 Maritime Supporting Facilities
11.4.4.1 Navigation Facilities
11.4.4.1.1 Lighthouses and Beacons
11.4.4.1.2 Buoys

11.4.4.1.3 Electronic Navigation Facilities
11.4.4.2 Emergency Search and Rescue Facilities
11.4.4.2.1 U.S. Coast Guard Marine Emergency Response Facilities
11.4.4.2.2 State and Local Marine Emergency Response Facilities
11.4.5 Other Maritime Facilities
11.5 MASS TRANSIT
11.5.1 Rail Mass Transit
11.5.1.1 Rail Transit Cars
11.5.1.1.1 Heavy Rail Transit
11.5.1.1.2 Light Rail Transit
11.5.1.1.3 Commuter Rail
11.5.1.1.4 Other Rail Transit
11.5.1.2 Rail Transit Passenger Stations
11.5.1.3 Rail Transit Rights of Way
11.5.1.3.1 Rail Transit Track
11.5.1.3.2 Rail Transit Bridges
11.5.1.3.3 Rail Transit Tunnels
11.5.1.4 Rail Transit Yards
11.5.1.5 Rail Transit Dispatch and Operations Control Centers
11.5.1.6 Rail Transit Communications Centers
11.5.1.7 Rail Transit Signaling Facilities and Equipment
11.5.2 Bus Mass Transit
11.5.2.1 Transit Bus Vehicles
11.5.2.2 Transit Bus Routes
11.5.2.3 Transit Bus Terminals
11.5.2.4 Transit Bus Stops
11.5.2.5 Transit Bus Garages
11.5.2.6 Transit Bus Dispatch and Operations Control Centers
11.5.2.7 Transit Bus Communications Centers
11.5.3 Other Mass Transit Systems
11.6 PIPELINES
11.6.1 Crude Oil Pipelines
11.6.1.1 Crude Oil Pipeline Components
11.6.1.2 Crude Oil Pipeline Pumping Stations
11.6.1.3 Crude Oil Pipeline Control Centers
11.6.1.4 Crude Oil Storage
11.6.1.5 Crude Oil Pipeline Hub
11.6.2 Petroleum Product Pipelines
11.6.2.1 Petroleum Product Pipeline Components and Interconnects
11.6.2.2 Petroleum Product Pipeline Pumping Stations
11.6.2.3 Petroleum Product Pipeline Control Centers
11.6.2.4 Petroleum Product Storage
11.6.3 Natural Gas Transmission Pipelines
11.6.3.1 Natural Gas Transmission Pipeline Components and Interconnects
11.6.3.2 Natural Gas Transmission Pipeline Compressor Stations
11.6.3.3 Natural Gas Transmission Pipeline Control Centers
11.6.3.4 Natural Gas Transmission Storage
11.6.3.5 Natural Gas Pipeline Hub
11.6.3.6 Natural Gas Receipt/Delivery Metering Stations
11.6.3.7 Liquefied Natural Gas Storage (Terminal)
11.6.4 Natural Gas Distribution
11.6.4.1 City Gate Stations
11.6.4.2 Natural Gas Distribution Pipeline Networks
11.6.4.3 Natural Gas Distribution Control and Dispatch Centers
11.6.4.4 Natural Gas Distribution Storage
11.6.5 Liquid Natural Gas (LNG) Facility
11.6.5.1 LNG Facility – Terminal (Marine)
11.6.5.2 LNG Facility – Liquefaction + Vaporization
11.6.5.3 LNG Facility – Vaporization
11.6.6 Other Pipelines
11.6.6.1 Other Pipeline Components
11.6.6.2 Other Pipeline Pumping Stations
11.6.6.3 Other Pipeline Control Centers
11.6.6.4 Other Pipeline Terminals
11.6.7 Other Pipeline Facilities
11.7 REGULATORY, OVERSIGHT, AND INDUSTRY ORGANIZATIONS
11.7.1 Federal Transportation Agencies
11.7.2 State and Local Transportation Agencies
11.7.3 Transportation Industry Organization

Appendix 6: Protocols and Processes for Assessing Effectiveness and Compliance

This appendix addresses specific requirements of Executive Order 13416, Strengthening Surface Transportation Security. The protocols and processes contained herein describe the Transportation Systems Sector's approach to the assessments required in paragraph 3 of the order. These processes will be refined as the measurement procedures associated with the NIPP and the Transportation Systems SSP are defined.

Protocol for Determining the Effectiveness of Information-Sharing Mechanisms

The information-sharing process is designed to communicate both actionable information on threats and incidents, and information pertaining to overall Transportation Systems Sector status (e.g., plausible threats, vulnerabilities, potential consequences, incident situation, and recovery progress). This is accomplished through the collection, production, and sharing of information that enables timely and effective decisionmaking so that owners and operators, States, localities, tribal governments, and other security partners can assess risks, make appropriate security investments, and take effective and efficient protective actions.

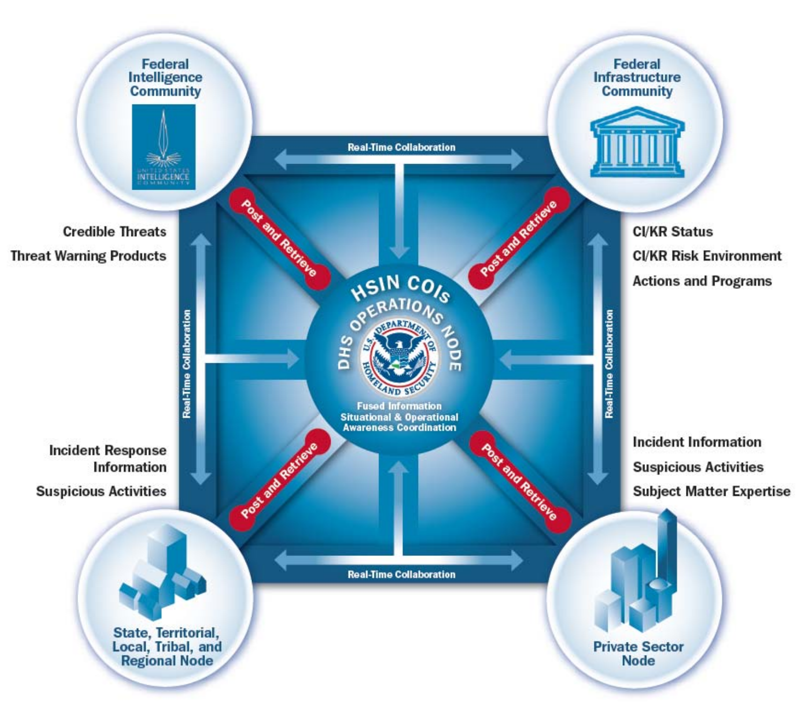
The effective implementation of the NIPP and the Transportation Systems SSP is predicated on active participation by government and private sector security partners in robust multi-directional information sharing. When the Nation's surface transportation owners and operators have a comprehensive picture of threats to the transportation system and its CI/KR and participate in the multi-directional information flow, their ability to assess risks, make prudent security investments, and take protective actions is substantially enhanced. Similarly, when the government is equipped with an understanding of private sector information needs, it can adjust its information collection, analysis, synthesis, and dissemination activities accordingly.

The NIPP and Transportation Systems SSP information-sharing approach constitutes a shift from a strictly hierarchical to a networked model, allowing distribution and access to information both vertically and horizontally, as well as the ability to enable decentralized decisionmaking and actions. The objectives of the networked approach are to:

- Enable secure multi-directional information sharing between and across government and industry that focuses, streamlines, and reduces redundant reporting to the greatest extent possible;
- Implement a common set of communications, coordination, and information-sharing capabilities for all security partners;
- Provide security partners with a robust communications framework tailored to their specific information-sharing requirements, risk landscape, and protective architecture;
- Provide security partners with a comprehensive common operating picture that includes, but is not limited to, timely and accurate information about natural hazards, general and specific terrorist threats, incidents and events, impact assessments, recommended security guidelines, lessons learned, and best practices;

- Provide security partners with timely incident reporting and verification of related facts that the Transportation Systems Sector and other CI/KR owners and operators can use with confidence when considering how evolving incidents might affect their security posture;
- Provide a means for State, local, tribal, and private sector security partners to be integrated, as appropriate, into the intelligence cycle, to include providing inputs to the intelligence requirements development process;
- Enable the flow of information required for security partners to assess risks, conduct risk management activities, invest in security measures, and allocate resources; and
- Protect the integrity and confidentiality of sensitive information.

Figure A7-1: NIPP Information-Sharing Framework



Protocol for Measuring the Effectiveness of Security Information Sharing

Measuring the effectiveness of information sharing requires a multi-dimensional assessment approach that can be implemented by actively engaging the Transportation Systems Sector's security partners. Effective information sharing is an outcome of a number of interrelated, complementary, and dynamic capabilities within the sector that can be best assessed and evaluated by developing metrics against each of the information-sharing dimensions. A sample of some of these dimensions includes the following:

- **Stakeholders**: The interactions of participants involved in an information-sharing initiative;
- **Data/Information**: The quality and pertinence of the information provided to the stakeholders;
- **Business Processes**: The timeliness and execution of the information-sharing initiative; and

- **Technology**: The technological capabilities and appropriate use of tools and mechanisms to implement the information-sharing initiative.

Sector security partners working through the GCCs and SCCs will identify and define the key information-sharing dimensions that will then be used to frame the assessment approach. The timeliness of information exchange through the most critical information-sharing mechanisms will be assessed on an annual basis.

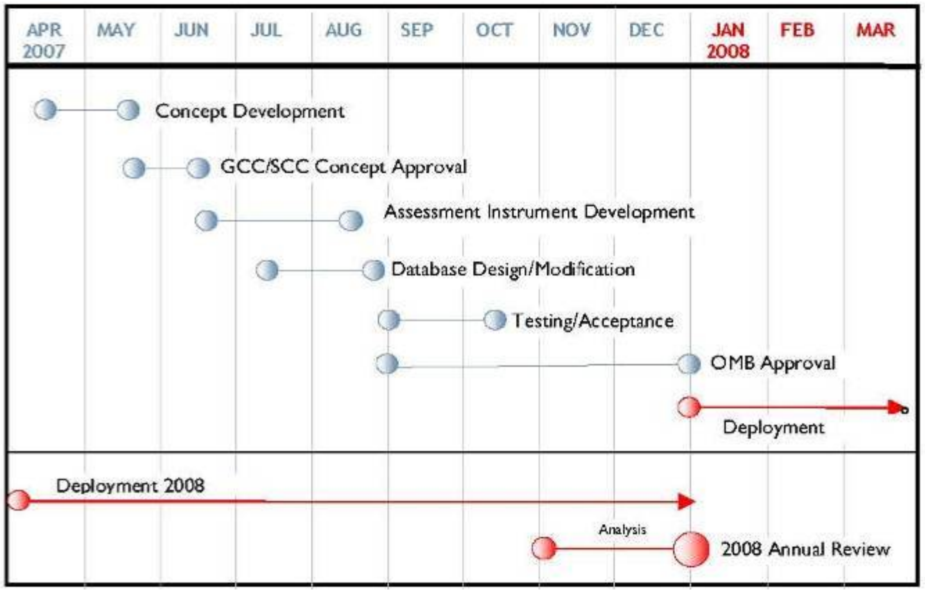
The protocol for measuring effectiveness will align with the Information Sharing Environment Implementation Plan developed under the requirements of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), and with the NIPP and the Transportation Systems SSP measurement requirements. Process measurement data will also be used where the sector has access to such information.

Consistent with Executive Order 13416, Strengthening Surface Transportation Security, this protocol will initially focus on timeliness since the determination of future effectiveness measures will be determined and developed at the user's level (GCCs/SCCs) to incorporate metrics and other evaluation procedures to measure progress and assess the effectiveness of information shared.

Schedule for Annual Information-Sharing Mechanism Effectiveness Assessment

The schedule proposed in the table below will be adjusted, as necessary, at the discretion of the sector's security partners through the GCC and SCC venues to conform to the information process metrics and timelines of the NIPP and Transportation Systems SSP implementation initiatives and the requirements of the information-sharing environment.

Figure A7-2: Annual Schedule for Developing and Reviewing Information Sharing Effectiveness Measures



Process for Evaluating Compliance With and the Need for Revisions of Security Guidelines and Requirements

The security of the Nation's surface transportation is vital and both the public and private sectors share responsibility for its security. More than 85 percent of the Nation's surface transportation assets lie in private hands and there can be no real security for the Nation without highly effective public/private cooperation.

The Federal Government in partnership with the owners of transportation systems and acting through TSA will continue to seek the development of cooperative security measures for the Nation. These partnerships have and will continue to develop voluntary security guidelines. The current set of security guidelines are identified in the modal annexes of the Transportation Systems SSP. In the future, further voluntary guidelines may be developed by TSA in cooperation with industry, its leadership, its communities of interest, modal GCCs, SCCs, the public, and others.

Guidelines may form the basis for rulemaking should rulemaking be seen as necessary. In the way ahead, adherence to cooperatively developed guidelines will be provided by owner certification. To ensure adherence, TSA will review owner-provided certifications and provide random field audits of a statistically significant portion of those certifications by TSA inspectors or their agents.

When the needs of the Nation demand mandatory security requirements because of acts of terrorism, failure to meet voluntary guidelines, threat information, congressional mandates, court decisions, Executive Orders, petitions for rulemaking, or the like, TSA will act according to its responsibility granted under Public Law 107-71 and seek remedy under its rulemaking authority.

The continuing effectiveness of measures taken to ensure security within the Nation's transportation system requires review as the threats and measures of terrorism continually evolve. Under the guidelines of the Transportation Systems SSP, using NIPP metrics to compare performance to goals, security partners will adjust and adapt the Nation's CI/KR approach to account for progress achieved, as well as for changes in the threat environment. Among actions to ensure the continuing effectiveness of security measures, TSA and the Transportation Systems Sector communities of interest, as outlined in their Transportation Systems SSP modal plans, provide a schedule to meet regularly as GCCs and SCCs to review all security measures in place.

Homeland
Security